PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-085811
(43)Date of publication of application : 25.03.1994

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/00
H04Q 3/545

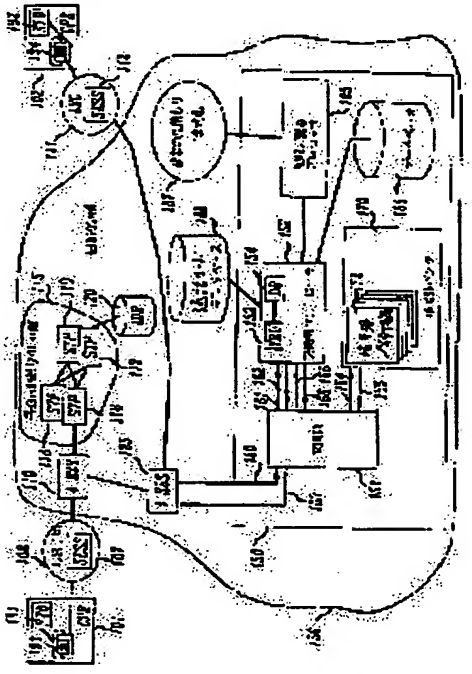
(21)Application number : 04-351390
(22)Date of filing : 08.12.1992

(71)Applicant : AMERICAN TELEPH & TELEGR CO <ATT>
(72)Inventor : BULFER ANDREW F
KAPLAN MICHAEL M
MCNAIR BRUCE E
WEGRZYNOWICZ CAROL A

(30)Priority
Priority number : 91 803809 Priority date : 09.12.1991 Priority country : US

(54) METHOD AND SYSTEM FOR MAKING COMMUNICATION VIA EXCHANGE NETWORK AVAILABLE, METHOD FOR PROVIDING SECURITY FUNCTION TO SECURITY NODE AND EXCHANGE NETWORK, METHOD FOR PROCESSING ENCRYPTED COMMUNICATION, AND METHOD FOR PROVIDING SECURITY COMMUNICATION

(57)Abstract:
PURPOSE: To provide comparatively secure communication even when parties concerned of a call use a security device with different protocols and algorithms by placing a security node that explains a security signal received from a CPE before information is delivered to a called party in a non-encryption form.
CONSTITUTION: A security node 150 placed to an electric communication network connecting a caller and a called party has a converter 151, a controller 152 converts received encrypted voice and data signals into information or non-encryption information encrypted by a different form in cooperation with the exchange 151 and conducts the inverse conversion. The controller 152 gives a control signal relating to the type of selected encryption used by the caller to the exchange 151. In the case of calling a hunt group, a proper encryption device such as 172 is selected and the controller 152 is used for the processing. The call signal is fed from the controller 152 to the exchange 151 through a conductor wire 168, and reverse communication, that is, communication from the called party 102 to the caller 101 takes the same path when the call path is once formed by the exchange 151 and an encryption device 172 in the return direction is used.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－85811

(43)公開日　平成6年(1994)3月25日

(51)Int. Cl.[5]	識別記号	庁内整理番号	FI		技術表示箇所
H04L	9/00				
	9/10				
	9/12				
		7117－5K	H04L	9/00	Z
		8529－5K		11/00	

審査請求　有　請求項の数25　(全23頁)　最終頁に続く

(21)出願番号　特願平4-351390

(22)出願日　平成4年(1992)12月8日

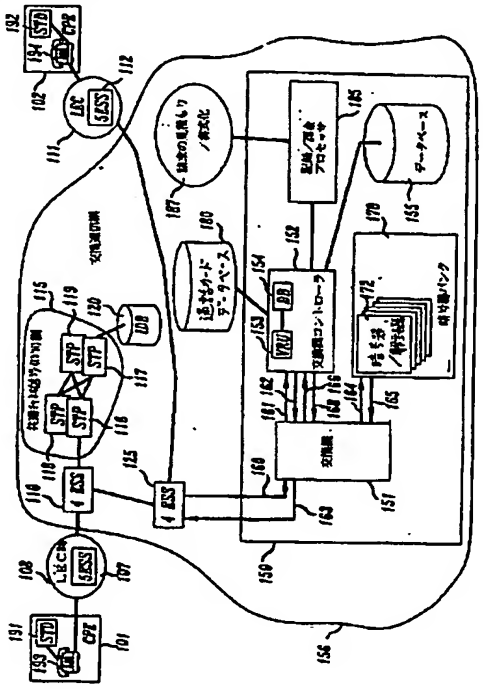
(31)優先権主張番号　803809
(32)優先日　1991年12月9日
(33)優先権主張国　米国（US）

(71)出願人　390035493
アメリカン　テレフォン　アンド　テレグラフ　カムパニー
AMERICAN TELEPHONE AND TELEGPAPH COMPANY
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32
(74)代理人　弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】交換網を介する通信を可能とする方法およびシステム、安全ノード、交換網に安全機能を与える方法、暗号化通信を処理する方法、ならびに安全な通信を与える方法

(57)【要約】
【目的】　呼の両当事者がプロトコルおよびアルゴリズムの異なる安全装置を用いたり、安全装置を一方しか持たない場合も、比較的安全な通信を与える。
【構成】　発呼者と被呼者を接続する電気通信網に配置された安全ノードが、第１の形式で暗号化された情報（音声、データ等）を(a)異なる形式で暗号化された情報または(b)非暗号化情報に変換し、またこの逆変換も行う。安全ノードは通信網に接続された任意の場所からアクセスできる。呼またはメッセージに安全ノード経由の経路を与え、安全ノードに適切な制御信号を与えることにより、当事者間の伝送経路の部分のみにおいて情報を暗号化し、他の部分は情報をクリア（暗号化しない）とすることができる。または、異なる暗号アルゴリズムを用いて、経路の異なる部分で情報を暗号化することもできる。



1

【特許請求の範囲】

【請求項１】　交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、

前記発呼者によって発信され前記被呼者に宛てられ且つ暗号化情報を前記通信網に適用するＣＰＥ（加入者構内装置）と、

前記交換網に配置されていて、前記ＣＰＥから受信した前記の暗号化情報を該情報が前記被呼者に非暗号化形式で伝達される前に解読するように構成された安全ノードとを備え、

前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信がクリア（非暗号化）であることを特徴とする交換網を介する通信を可能とするシステム。

【請求項２】　前記安全ノードが、

交換機と、

複数の暗号解読器と、

前記の暗号化情報に前記暗号解読器のうちの特定の解読器への経路を設定するために前記交換機を制御する制御手段とを備えたことを特徴とする請求項１記載のシステム。

【請求項３】　前記制御手段が、

データベースと、

前記ＣＰＥにおいて使用される暗号の型を判定する手段と、

前記暗号型の各々を前記暗号解読器のうちの特定の解読器に関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項２記載のシステム。

【請求項４】　発呼者から暗号化情報を受信する手段と、

前記の暗号化情報に、対応する非暗号化情報を生成するための解読器を通して経路を与える手段と、

前記の非暗号化情報を前記被呼者に送る手段とを備えた交換通信網に配置されることを特徴とする安全ノード。

【請求項５】　交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、

前記発呼者によって発信され前記被呼者に宛てられ且つ非暗号化情報を前記通信網に適用するＣＰＥ（加入者構内装置）と、

前記交換網に配置されていて、前記ＣＰＥから受信した前記の非暗号化情報を該情報が前記被呼者に暗号化形式で伝達される前に暗号化するように構成された安全ノードとを備え、前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信が暗号化されていないことを特徴とする交換通信網を介する通信を可能とするシステム。

【請求項６】　前記安全ノードが、

交換機と、

複数の暗号器と、

2

前記の非暗号化情報に前記暗号器のうちの特定の暗号器への経路を設定するために前記交換機を制御する制御手段とを備えたことを特徴とする請求項５記載のシステム。

【請求項７】　前記制御手段が、

データベースと、

前記被呼者によって使用される暗号の型を判定する手段と、

前記暗号型の各々を前記暗号器のうちの特定の暗号器に関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項６記載のシステム。

【請求項８】　交換通信網に配置され；発呼者から非暗号化情報を受信する手段と、

前記の非暗号化情報に、対応する暗号化情報を生成するための複数の暗号解読器のうちの選択された解読器を通して経路を与える手段と、

前記の暗号化情報を前記被呼者に送る手段とを備えたことを特徴とする安全ノード。

【請求項９】　交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、

前記発呼者によって発信され前記被呼者に宛てられ且つ暗号化情報を前記通信網に適用する第１のＣＰＥ（加入者構内装置）と、

前記交換網に配置されていて、第１の暗号化アルゴリズムを用いる前記ＣＰＥから受信した情報を前記第１の暗号化アルゴリズムとは異なる第２の暗号化アルゴリズムを用いて暗号化情報に変換するように構成された安全ノードと、　前記安全ノードから前記被呼者に宛てられ暗号化形式の変換された情報を受信する第２のＣＰＥとを備え、前記呼経路の少なくとも第１の部分にわたる通信が第１の暗号化アルゴリズムを用いて暗号化され、かつ前記呼経路の少なくとも第２の部分にわたる通信が第２の暗号化アルゴリズムを用いて暗号化されることを特徴とする交換通信網を介する通信を可能とするシステム。

【請求項１０】　前記安全ノードが、

交換機と、

複数の暗号器および暗号解読器と、

前記の暗号化情報に前記の暗号器および暗号解読器のうちの特定のものを通る経路を与えるために前記交換機を制御する制御手段とを備えたことを特徴とする請求項９記載のシステム。

【請求項１１】　前記制御手段が、

データベースと、

前記の第１および第２のＣＰＥで使用される暗号の型を判定する手段と、

前記暗号型の各々を前記の暗号器および暗号解読器のうちの特定のものに関係付けて前記データベースに記憶されている情報を検索する手段とを備えたことを特徴とする請求項１０記載のシステム。

3

【請求項１２】　交換通信網に配置され；発呼者から第１の暗号化形式を用いて暗号化情報を受信する手段と、
前記の暗号化情報に、対応するクリアな情報を生成するための解読器を通して経路を与える手段と、
前記の対応するクリアな情報に、第２の暗号化形式を用いて暗号化情報を生成するための暗号器を通る経路を与える手段と、
前記の暗号化情報を前記被呼者に送る手段とを備えたことを特徴とする安全ノード。

【請求項１３】　交換通信システムを通る経路が選択される暗号化通信を処理するために；異なる暗号化／暗号解読アルゴリズムを用いて通信を暗号化／解読するようにそれぞれ構成された複数の異なる型の暗号器と、
入って来る通信に、与えられた信号メッセージに応じて複数のハント・グループの１つへの経路を与えることにより、前記ハント・グループの何れに経路設定される通信も特定の型の前記暗号器のうちの利用できるものに接続されるように構成されたＰＢＸと、
前記の入って来る呼に用いられている特定の暗号化／暗号解読アルゴリズムにしたがって前記信号メッセージを前記ＰＢＸに与える手段とを備えたことを特徴とする安全ノード。

【請求項１４】　交換通信網を含む呼経路を介して発呼者と被呼者との間で通信を行うために；加入者構内装置（ＣＰＥ）で前記発呼者により発信され前記被呼者に宛てられ且つ暗号化情報を前記交換通信網に適用するステップと、
前記交換通信網に配置された安全ノードにおいて、前記ＣＰＥから受信された前記の暗号化情報を、前記情報が前記被呼者に非暗号化形式で伝達される前に解読するステップとを備え、前記呼経路の少なくとも一部分にわたる通信が暗号化され、かつ前記呼経路の残りの部分にわたる通信がクリアであることを特徴とする交換網を介する通信を可能とする方法。

【請求項１５】　前記安全ノードが、交換器および複数の暗号解読器を備え、前記方法が、前記の暗号化情報を前記暗号解読器の特定の解読器に経路付けするように前記交換機を制御する制御ステップをさらに含むことを特徴とする請求項１４記載の方法。

【請求項１６】　前記制御ステップが、
前記ＣＰＥにおいて使用されている暗号の型を判定するステップと、
前記暗号型の各々を前記暗号解読器の特定のものに関係付けながらデータベースに記憶されている情報を検索するステップとを備えたことを特徴とする請求項１５記載の方法。

【請求項１７】　発呼者から暗号化情報を交換通信網の中に配置された安全ノードにおいて受信するステップと、
対応するクリアな情報を生成するために、前記ノードにある暗号解読器を通る経路を前記の暗号化情報に与えるステップと、
前記のクリアな情報を前記ノードから前記被呼者に送るステップとを備えたことを特徴とする交換網に安全機能を与える方法。

4

【請求項１８】　交換通信網を含む呼経路を介して発呼者と被呼者との間の通信を可能とするために、
前記発呼者によって発信され前記被呼者に宛てられ且つ非暗号化情報を第１の加入者構内装置（ＣＰＥ）から前記通信網に適用するステップと、
前記交換通信網に配置された安全ノードにおいて前記第１のＣＰＥから受信された前記の非暗号化情報を該情報が前記被呼者に暗号化形式で伝達される前に暗号化するステップとを備え、前記呼経路の少なくとも第１の部分にわたる通信が暗号化されず、前記呼経路の残りの部分にわたる通信が暗号化されることを特徴とする交換通信網を介する通信を可能とする方法。

【請求項１９】　特定の型の暗号器を用いる発呼者からの情報を交換通信網の中に配置された安全ノードにおいて受信するステップと、
対応するクリアな情報を生成するように構成された前記安全ノードにおける複数の暗号解読器の適切な解読器を通して前記の暗号化情報の経路選択を行うステップと、
前記のクリアな情報を前記ノードから前記被呼者に送るステップとを備えたことを特徴とする交換網に安全機能を与える方法。

【請求項２０】　交換通信システムを通る経路が選択される暗号化通信を処理するために；前記の暗号化通信をＰＢＸに適用するステップと、
異なる暗号化／暗号解読アルゴリズムを用いて通信を暗号化／解読するようにそれぞれ構成された複数の異なる型の暗号器の１つに向かい前記ＰＢＸを通る経路を前記通信に与えるステップと、
入って来る通信に、前記ＰＢＸに与えられる信号メッセージに応じてＰＢＸ内の複数のハント・グループの１つへの経路を与えることにより、前記ハント・グループの何れに向けて経路設定される通信も特定の型の前記暗号器の適切なものに接続されるステップと、
前記の入って来る通信に使用される特定の暗号化／暗号解読アルゴリズムにしたがって前記信号メッセージを前記ＰＢＸに与えるステップとを備えたことを特徴とする暗号化通信を処理する方法。

【請求項２１】　発呼者と被呼者との間に安全な通信を与えるために；前記発呼者および前記被呼者を接続する通信網においてクリアな通信経路を確立する確立ステップと、
安全な通信を開始したいという前記の両当事者のうちの一方による希望を表す信号を検出するために前記通信経路を監視するステップと、
前記通信経路の少なくとも一部分の通信をクリアから安

5

全に変換する変換ステップとを備えたことを特徴とする安全な通信を与える方法。

【請求項２２】　前記確立ステップが、前記発呼者から前記被呼者への呼に対し前記通信網に配置されたインテリジェント交換機を介する経路を与えるステップを含み、かつ前記変換ステップが、前記の一方の当事者によって使用される関係付けられた暗号化装置と互換性のある選択された暗号化装置を前記通信経路に挿入するように前記インテリジェント交換機を制御するステップを含むことを特徴とする請求項２１記載の方法。

【請求項２３】　前記の関係付けられた暗号化装置において使用される暗号化アルゴリズムの型を確認するために前記の一方の当事者に問い合わせるステップと、
前記の問い合わせに対する応答にしたがって前記の選択された暗号化装置を選ぶステップとをさらに備えたことを特徴とする請求項２２記載の方法。

【請求項２４】　安全な通信を与えたいという前記の両当事者の他方による希望を表す信号を検出するために前記通信経路を監視するステップ、および前記通信経路の残りの部分の通信をクリアから安全に変換するステップをさらに備えたことを特徴とする請求項２１記載の方法。

【請求項２５】　前記確立ステップが、前記発呼者から前記被呼者への呼に対し前記通信網に配置されたインテリジュント交換機を介する経路を与えるステップを含み、
前記変換ステップの各々が、前記の両当事者によって使用される関係付けられた暗号化装置と互換性のある選択された暗号化装置を前記通信経路に挿入するように前記インテリジェント交換機を制御するステップを含むことを特徴とする請求項２４記載の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、概して、音声、データ、ファクシミリ、ビデオ、およびその他の情報を伴う安全な通信に関する。

【０００２】

【従来の技術】資格のない人々が彼らのためのものではない音声、データ、ファクシミリ、ビデオ、またはその他の情報を傍受しアクセスすることができないように通信システムの安全性を高めることが過去数年にわたり非常に重要視されてきた。研究によれば、商業市場は自らの通信システムに対する脅威に十分気付いており、安全性が崩壊する可能性があるために危険であるようなビジネス・アプリケーションを明らかに意識している。このように関心が高まる理由は多数あり、会話の一部が空中を介して伝えられるために攻撃をより受けやすいセルラ電話の使用の増加、および電気通信網の他の部分---即ち、配線室（wiring closet）、接続箱（junction box）、マンホールまたは電柱の接続、ファクシミリ装

6

置、そして特にコードレスおよびセルラ式の電話---が安全の侵害を特に受ける可能性があるという事実もそうである。

【０００３】安全な通信への関心の高まりにもかかわらず、現在の安全技術にはいくつかの制限があり、安全な通信をしようと思うと発呼者も被呼者も暗号化された信号を共通のハンドシェイク・プロトコルおよび暗号化アルゴリズムを用いて送受信することのできる送受信両用の安全装備を備えなければならないという一般的な必要性もその１つである。そうでなければ、安全な通信は通常不可能である。このように、現時点では、セルラ電話を用い、それゆえにより高い安全性を望むような発呼者が適切な装備をしていない被呼者と通信することは一般に困難である。米国特許第4,972,479号（１９９０年１１月２０日に付与、発明者；アール・ダブリュ・トビアス(R.W.Tobias)）に記述された１つの例外において、この問題の解決を試みてはいるものの、加入者の構内に置かれた呼迂回装置を伴う複雑かつ非経済的な方法で行っている。別の状況では、セルラ電話の利用者は、移動電話交換局と暗号モードで通信することができ、移動電話交換局（ＭＴＳＯ＝mobiletelephone switching office）は、目的先への呼をクリアな（即ち、非暗号化）モードで完成させる。しかしながら、この種の構造の有用性には限度があり、ＭＴＳＯへのアクセスがそのＭＴＳＯのサービス範囲に物理的に位置する発呼者に限られていて、この範囲外の発呼者がＭＴＳＯの暗号設備を利用することはできない。さらに、ＭＴＳＯ環境において現在使用されている暗号構造では、１つの暗号アルゴリズムから別のものへの変換、および音声の呼以外の通信がサポートされていない。

【０００４】同様に、呼の発信者が安全な（即ち、暗号化可能な）電話を持っていない場合、それへの帰属が微妙と思われる領域において呼を受信している側が暗号化された情報を自らの局所的電話リンク（例えば、終端の中央局から加入者の構内まで）で受信することを保証することは一般に不可能である。さらに、仮に発呼者および被呼者の両方が安全な電話を持っていても、互いに正しく通信するためには、両者は、同じプロトコルおよびアルゴリズムを使用しなければならない。

【０００５】

【発明が解決しようとする課題】発明が解決しようとする課題は、呼の当事者の双方がハンドシェイク・プロトコルおよび暗号アルゴリズムの異なる安全装置を有する場合、または当事者の一方のみが安全装置を有する場合、安全な通信を行うことができないことである。

【０００６】

【課題を解決するための手段】本発明によれば、第１のフォーマットで暗号化された情報（これは、音声、データ、ファクシミリ、ビデオ、およびその他のタイプの呼またはメッセージでもよい）を（ａ）異なるフォーマッ

トで暗号化された情報、または（ｂ）非暗号化情報に変換したり、またはこの逆の変換をするように構成され、かつ発呼者および被呼者を接続する通信網に配置された安全なノード（以下において、「安全ノード」と称する）を用いることによって、両当事者の間で安全な通信を行うことができる。発呼者により発信され、前記の安全ノードを介して被呼者に送られる呼またはメッセージの経路選定を行うことによって、情報は、伝送経路の両当事者間の部分だけが暗号化され、伝送経路の他の部分は暗号化されないことがある。また、異なる暗号化アルゴリズムを用いて経路の異なる部分で情報が暗号化されることもある。これにより、発信端または終端において一方の当事者のみが安全装置を有する場合でも、通信路の安全でない部分への攻撃は可能であるがその可能性は小さいので、当事者は、比較的安全な通信が得られるサービスを受けることが可能となる。また、本発明では、異なるハンドシェイク・プロトコルおよび暗号化アルゴリズムによる安全装置を使用する当事者の間でも安全な通信が許される。安全な網サービス・ノードは一度に多くの利用者にアクセスされることがあるので、このサービスに関する費用は分担して小さくすることができる。

【０００７】

【実施例】図１は、本発明によって構成された安全ノード１５０の構造、および市内通信網および相互交換通信網の種々の要素とその構造との関係を示す。安全ノード１５０は、（ａ）伝送経路のある部分（例えば、発呼者とノード１５０との間の部分）で伝達される情報は安全にできる（暗号化できる）が、伝送経路の他の部分（例えば、ノード１５０と被呼者との間）で伝送される情報はクリアである（暗号化されない）ような通信、または（ｂ）発呼者とノード１５０との間の伝送経路の部分を伝達される情報が第１の暗号化アルゴリズムを用いて暗号化できる一方、ノード１５０と被呼者との間の伝送経路の部分で伝達される情報は第２の異なる暗号化アルゴリズムを用いて暗号化されるような通信を達成するように設計される。

【０００８】図１において、近い側の加入者構内装置（ＣＰＥ）１０１を使用している発呼者によって発信された通信は、遠い側のＣＰＥ１０２を使用している被呼者に宛てられ、またこの逆の場合もある。ここで用いる場合、「通信」には、音声、データ、ファクシミリ、ビデオ、またはその他の情報を伝えるアナログまたはデジタルの呼またはメッセージを含めても良い。以下において、通信を単に呼と称することがある。ＣＰＥ１０１および１０２は、それぞれ市販の安全電話ユニット（ＳＴＵ）----例えば、ＡＴ＆Ｔより入手可能なＳＴＵ-III電話、またはモトローラ（Motorola）もしくはジェネラル・エレクトリック（General Electric）のような販売会社から入手可能な別の安全端末など----を備えてもよい。あるいはまた、ＣＰＥ１０１および（または）ＣＰＥ１０２が、それぞれ安全電話装置（ＳＴＤ）１９１、１９２、即ち、関係付けられた電話１９３、１９４、またはファクシミリ装置、データ端末または他の通信装置へと接続する付属装置を備えても良い。尚、ＣＰＥ１０１またはＳＴＤ１９１がＣＰＥ１０２またはＳＴＤ１９２と同じ種類である必要はなく、事実、異なる暗号化アルゴリズムやハンドシェイク・プロトコルを用いる異なる製造業者から入手することも可能である。また、ＣＰＥ１０１またはＣＰＥ１０２の（両方ではなく）一方は、普通の（安全でない）端末または装置でもよい。

【０００９】以降の説明のために、ＣＰＥ１０１は、クリアか安全かを問わず出て行く（即ち、発呼者から安全ノードへの）呼および入って来る（即ち、安全ノードから被呼者への）呼を送受信するように構成されているものと仮定する。ＣＰＥ１０１の交換機により、装置が動作するモード（クリアまたは安全）を制御し、モードの変更は、交換機を操作することにより利用者の直接制御の下で局所的に行われたり、遠隔地で生成された信号に応じて行われたりする。データの入力を便利にするために、ＣＰＥ１０１にタッチ・トーン発生器およびキーパッドを備えて、ＬＥＤ表示ランプなどの表示指示器によって状態を利用者に示すことができる。安全からクリアの通信を最初に説明するので、すぐ後の説明のために、ＣＰＥ１０２が通常の電話機であると仮定する。

【００１０】安全ノード１５０への通信「アクセス」は、（ａ）ソフトウェアで定義されたネットワーク（ＳＤＮ）アクセス番号、または（ｂ）ＡＴ＆Ｔから利用可能なＭＥＧＡＣＯＭのようなプレミアム・サービスに関連した普通の旧式の電話サービス（ＰＯＴＳ＝plain old telephone service）番号、または（ｃ）８００番を使用するなどの便利なアクセス機構によって得ることができるが、説明のために、ＣＰＥ１０１を使用する発呼者は、1-８００-ＥＮＣＲＹＰＴのような所定の料金無料番号をダイヤルすることによってノード１５０へのアクセスを得るものと仮定する。この番号にダイヤルすると、呼は、発呼者を管轄する市内交換キャリア（ＬＥＣ）局１０８にある交換機１０７（例えば、ＡＴ＆Ｔから入手可能な電子交換機＃５ＥＳＳ(登録商標)）を通して、総括的に１５６として指定される交換通信網の一部である相互交換キャリア交換機１１０（一般に、ＡＴ＆Ｔの＃４ＥＳＳアクション・コントロール・ポイント（ＡＣＰ））へと経路選択されて送られる。交換機１１０は、これに応じて、信号メッセージを（通常はＣＣＳ７信号フォーマットで）生成し、これを相互に接続された複数の信号転送点（ＳＴＰ＝signal transfer point）１１６、１１７を含む共通チャネル信号（ＣＣＳ）網１１５を通して、発呼者の加入計画により着信ワッツ(InWATS)データベース（ＩＤＢ）１２０またはソフトウェアで定義されたネットワークにおける網制御点（ＮＣＰ）へと経路選択して送る。ＩＤＢ１２０は、ダイヤルされ

たそれぞれの８００番に対するレコードを収容し、ダイヤルされた番号に関係付けられた経路選択番号（これは、交換機１１０に送り返される）を生成するために参照動作を行う。次に、交換機１１０は、経路選択番号に応じて、その呼を安全ノード１５０へと経路選択して送るが、通常は交換通信網１５６の他の構成要素を通して送り、このとき別の＃４ＥＳＳ交換機１２５を含んでも良い。また、ＬＥＣ局１０８には発呼者を図１に示したように直接接続しても、ＰＢＸ交換機または他の加入者構内装置（ＣＰＥ）（図示せず）を介して接続しても良い。さらに、ＣＰＥ１０１と安全ノード１５０との相互接続には、他のアクセス構造および信号構造を使用しても良い。

【００１１】安全ノードにおいて呼が受信されると、そのノードは、ダイヤルされた番号およびＣＰＥ１０１を識別する自動番号識別（ＡＮＩ）情報が入ったＣＣＳメッセージも交換機１０７、１１０、または１２５から受信する。しかしながら、そのような情報の利用可能性は、ＬＥＣ局１０８およびネットワーク１５６によって使用されている交換機および信号装置の能力に依存する。次の説明のために、発呼者の情報は発呼者に催促することなしには利用できないものと仮定する。

【００１２】図１に示したように、安全ノード１５０は交換機１５１を備えている。この交換機は、例えば、ＡＴ＆Ｔより入手可能なDefinity（商標）デジタルＰＢＸであり、トランク１６０上で受信した入接続呼を線群１６１の中の１つの線を介して交換機コントローラ１５２の利用可能なポートに接続するように構成されている。また、交換機１５１は、呼を線群１６４経由で暗号器バンク１７０の中で利用可能な暗号器に接続するように構成されている。コントローラ１５２は、例えばＡＴ＆Ｔより入手可能なConversant（登録商標）システムであり、内部のデータベース（ＤＢ）１５４に記憶された原稿に従って発呼者に音声のプロンプトを送信できる音声応答ユニット（ＶＲＵ）１５３を含む。また、コントローラ１５２は、それ自体でまたは交換機１５１と連携して他の種々の機能を果たす。例えば、プロンプト送信に応じて発呼者が入力した情報を受信し、これをデータベース１６４から検索した情報との関連において論理的な処理をすることができる。このような情報は、通常ＣＰＥ１０１の一部であるタッチ・トーン・ダイヤル・パッドを用いるか、またはキーボードもしくは他の別個の入力装置によって、発呼者が入力することができる。場合によっては、情報を音声の応答として入力し、「音声からテキストに」処理する機能を用いて翻訳できることもある。さらに、コントローラ１５２は、交換機１５１と連携して、（ａ）ダイヤル数列を生成して交換機１５１に適用することによって呼を開始する（または開始するように交換機１５１に指示する）こと、（ｂ）いくつかの入力で呼を同時に受信し処理すること、さらに（ｃ）入接続呼および出せつぞく呼を共にブリッジする（またはブリッジするように交換機１５１に指示する）ことが、可能である。また、コントローラ１５２は、発呼者または被呼者によって呼経路に印加される制御信号を検出し、それに基づいて動作するために所定の時間または期間だけ呼経路に留まることができる。以上の機能は、前記のConversantシステムおよび他の業者より入手可能な同様のシステムにおいてもすべて利用することができる。

【００１３】安全からクリアの通信（即ち、ＣＰＥ１０１と安全ノード１５０との間の安全、およびその安全ノード１５０と被呼者との間のクリア）を実現しようとしてノード１５０の番号（例えば、1-800-ENCRYPT）をダイヤルした発呼者から呼を受信した場合に、コントローラ１５２において取られる処置を図２に流れ図のかたちで示し、次のように要約する。

【００１４】呼の受信時（ステップ２０１）に、交換機コントローラ１５２は、その呼の完成に必要な情報を求めて発呼者にプロンプトを出す（ステップ２０３）。この情報には、発呼者が加入者であることを確認する「ログイン」などの情報、発呼者の同一性を確認する「パスワード」などの情報、および例えばＣＰＥ１０２の電話番号などの被呼者を識別する情報も含まれる。

【００１５】処理におけるこの時点において、発呼者によって用いられる暗号の種類を識別する情報も音声プロンプトに応じてコントローラ１５２で受信することがある。しかしながら、暗号化を開始する前に交わされる「安全伝送開始」信号に暗号の種類を示す符号を含めることなどによって前記の情報の提供を自動化する方が好ましい。しかし、さらに詳細に後述するように暗号の種類は後続の設定過程のある時点で得るようにしてもよい。以下の説明のために、暗号の種類はステップ２０６において獲得して、データベース１５４に格納するものと仮定する。異なる暗号化アルゴリズムを取り入れて使用する種々の異なるＣＰＥを使用する加入者を支援するようにノード１５０が構成されているので、いずれの場合も「種類の情報」は必要となる。従って、ノード１５０において適切な処理を実施するためには、発呼者によって使用される暗号の特定の種類の詳細が必要となる。

【００１６】コントローラ１５２は、発呼者入力情報を受信すると、その発呼者が資格のある利用者かどうかを知るためにデータベース１５５を調べる（ステップ２０７）。資格がない場合、コントローラ１５２は、ステップ２０９において終了の告知を行うのに対し、資格がある場合、残りのプロンプトに応じて入力される情報を続けて収集する。さらに、コントローラ１５２は、課金処理を開始するために発呼者の識別情報および被呼者の情報を記録／課金プロセッサ１８５に送る（ステップ２１１）。プロセッサ１８５は、以降の一連の課金のために呼の詳細を記録している自動課金評価／書式化システム

１８７と周期的に通信を行う。呼の詳細には、通話の日付、時刻および長さ、呼び出された番号などが含まれる。課金処理を、ノード１５０に関係する呼設定および暗号化の「主な」処理とは関わりなく続くように図２に示す。

【００１７】コントローラ１５２が、ＣＰＥ１０１において使用されている暗号の型を判定すると、ＣＰＥ１０１で生成された暗号化された信号を効率的に処理（即ち、解読）できる暗号アルゴリズムを使用する暗号器バンク１７０のバンク内部で選択された暗号器に関係付けられたハント・グループの指定を判断するためにデータベースの参照動作が行われる（ステップ２１５）。同じ暗号型を用いている呼は幾つか同時に処理することができるので、暗号器バンク１７０には、そのようないくつかの暗号器が含まれ、それらの各々が同じハント・グループにおいて個別のアクセス番号を持っている。

【００１８】次に、コントローラ１５２は、発呼者によって使用されている選択された暗号の型に関係付けられたハント・グループを表す制御信号（一般に、トーン信号）を交換機１５１に結合する。ハント・グループが呼び出されると、次に利用可能な適切な型の暗号器（例えば、図１の暗号器１７２）が交換機１５１によって選択される。しかし、選択された型の暗号器が利用できない場合（ステップ２１７）、処理は終了する（ステップ２０９）。

【００１９】特定の暗号器が選択された場合、（ＣＰＥ１０１において生成された呼に関する）その入力端が、導線１６４によって交換機１５１に接続される（ステップ２１９）。順方向、即ちＣＰＥ１０１からＣＰＥ１０２の方向には、実際に暗号器１７２は、ＣＰＥ１０１で暗号化された呼を解読するように動作して、呼はＣＰＥ１０２からノード１５０までクリアに展開することができる。

【００２０】暗号器バンク１７０の中の暗号器はそれ自体に通信信号能力はほとんど備えていないので、暗号器１７２を含む各暗号器は、信号処理をコントローラ１５２によって行うことができるように暗号器の（ＣＰＥ１０１で生成された呼に関する）出力端が交換機１５１の導線側の端に接続されるように構成することができる。具体的には、暗号器１７２が選択されると、その出力端は、交換機１５１の導線１６５に接続され、これによって、ダイヤル・トーンがコントローラ１５２に供給される。

【００２１】交換機コントローラ１５２は、ダイヤル・トーンを受信すると、これに応じて交換機１５１に加えられるダイヤル・トーンを生成し、その交換機にコントローラ１５２への第２の呼を開始させる（ステップ２２１）ように構成される。この呼（導線１６６を介して交換機１５１からコントローラ１５２に展開される）は、呼設定処理が完了した後にコントローラがクリア・モードの（即ち、非暗号化）呼を引き続き監視できるようにするので、望ましいものである。さらに詳細に後述するように、コントローラ１５２による第１の接続（呼の設定が完了した後、切断される）により、コントローラが呼の道筋にあたる位置に置かれるので、（クリアではなく）暗号化された音声／データが受信される。

【００２２】ここで、コントローラ１５２は、ＣＰＥ１０２の呼を完成させる位置にある。呼を完成させるために、入接続呼（即ち、ＣＰＥ１０１から暗号器１７２を介してコントローラ１５２に至る呼）を保留し、以前に与えられデータベース１５４に格納されていた被呼者の番号への新たな呼を開始する（ステップ２２３）。この呼の経路は、コントローラ１５２から交換機１５１へ導線１６８を介して与えられる。この呼は、交換機１５１からトランク１６３を介して交換機１２５に経路付けされ、さらに通常の呼設定および信号授受の手順を用いて通信網経由で意図する伝送先のＣＰＥ１０２まで経路付けされる。安全ノード１５０から被呼者への出口は、ＳＤＮ（ソフトウェア定義ネットワーク）のMEGACOM（登録商標）またはその他のサービス（ＡＴ＆Ｔから入手可能なPROWATS、WATS即ちビジネス長距離）によって与えられる。通信網１５６とＣＰＥ１０２との間の通信は、一般に第２のＬＥＣ局（終端用の＃５ＥＳＳ交換機１１１を備えている）によって行われる。

【００２３】発呼者が応答すると、応答指示が交換機１２５で検出され、交換機１５１を通してコントローラ１５２に渡される。コントローラ１５２は、これに応じてコントローラ１５２への呼（導線１６１上）をコントローラ１５２からの呼（導線１６２上）にブリッジするよう交換機１５１に合図するように構成されている。これにより、コントローラ１５２の「出現」が呼経路から１つ除去されるが、第２の出現がそのまま残る。これによって、コントローラ１５２は、端から端までの接続が行われた後、制御信号（タッチ・トーン信号または音声で、暗号化されているものよりクリアなものが多い）の発生を知るために引き続き呼を「監視」することができるので、呼の進行中に以下に述べる他の何らかの動作を行うことができる。

【００２４】逆方向、即ち被呼者（ＣＰＥ１０２）から発呼者（ＣＰＥ１０１）への通信は、呼経路が交換機１５１で一旦設定されると、同じ経路をたどり、戻りの方向に対する（暗号解読ではなく）暗号ユニットとして暗号器１７２を使用する。

【００２５】発呼者とノード１５０との間の安全な通信を実現するために使用されるトレーニング・シーケンスを説明する前に、呼の設定過程を図３に関連した別の形式で説明する。図３において、図１にある構成要素に対しては同じ表示を使用しているが、呼の流れは「直線的に」示してある。即ち、交換機１５１およびコントローラ１５２が複数回現れるのを一括していない。

【００２６】図３において、ＣＰＥ１０１によって開始された呼は、例えば交換機１０７、１１０および１２５を含む市内および市外の通信網（図３には図示せず）を通る経路により送られ、交換機１５１の第１の入力ポート３０１に達し（ステップ２０１）、さらにこれにより、その出力ポート３０２を介してコントローラ１５２の第１の入力ポート３１１へと経路選択されて送られる。ＣＰＥ１０１において行われる暗号化の種類を判定するために十分な情報をコントローラが得た後（ステップ２０３、２０５）、コントローラ１５２によって暗号器バンク１７０にある暗号器の中の１つ（例えば、暗号器１７２）に接続が行われる（ステップ２０７、２１５、２１７）。この接続は、（１）コントローラ１５２によってその出力ポート３１２において交換機１５１の利用可能な入力を捉え、かつ（２）適切な種類の暗号器に関係付けられたハント・グループ番号をダイヤルすることによって、行われる。この接続により、交換機１５１は呼を出力ポート３０４から暗号器１７２へと経路付けして送る（ステップ２１９）ことになる。

【００２７】暗号器１７２の出力側は、交換機１５１の入力ポート３０５に接続され（ステップ２２１）、これによって、ダイヤル・トーンがコントローラ１５２に送り返される。コントローラ１５２は、このダイヤル・トーンの受信に応じて、呼をその着信先に接続するために必要な信号（即ち、各桁の数字）をポート３１２からコントローラ１５２を通る第２の接続によって出力する（ステップ２２３）。この接続を確立する方法は幾つかあるが、次の手順が好ましい。まずポート３１２からのデジタル出力により交換機１５１に呼を開始させることにより、その入力ポート３０５を出力ポート３０６に接続し、この出力ポートはコントローラ１５２の第２の入力ポート３１３に接続される。コントローラ１５２は、出力信号（数字）を受信し、ダイヤルされた番号を表す制御信号を出力ポート３１４から交換機１５１の利用可能な入力ポート３０７に与えることにより新たな呼を交換機１５１によって開始する。この呼が開始されるのは、交換機１５１がポート３０７を交換通信網における交換機１２５に接続された出力ポート３０８に接続するときである。

【００２８】ＣＰＥ１０２を使用する被呼者から応答指示を受信すると、ＣＰＥ１０１からノード１５０を通して被呼者のＣＰＥ１０２までクリアな通信路が形成される。この時、コントローラ１５２は、交換機１５１にポート３０１における呼の入力をポート３０４における呼の出力と共にブリッジするように合図する（ステップ２２５）。これにより、コントローラ１５２が１回出現する周囲にバイパスが設置されるが、呼を監視し（ステップ２２７）、制御信号または呼ステータスの状態を検出し、これに応じて、他の種々の呼設定および（または）維持機能を実行するために、このコントローラの第２の出現が呼経路のクリアな部分に残ることが許される。

【００２９】図２との関連で説明した処理により、ＣＰＥ１０１とＣＰＥセル１０２との間に安全なノード１５０によるクリアな通信路が設置される。呼の期間中に時として、発呼者がＣＰＥ１０１とノード１５０との間の呼の部分を暗号化することに決めることがある。ＣＰＥ１０１と安全ノード１５０との間の通信をクリアから暗号化へと切り替えることを可能にするトレーニング・シーケンス処理を図４に示す。同図は、図３に関して続けて読むべきである。発呼者は、暗号通信を始めたいと思った場合、その意図を着信側に知らせたのち、例えばＣＰＥ１０１の「安全通話」ボタンを押す（ステップ４０１）などによりＣＰＥ１０１内部の暗号ユニットにきっかけを与えてモデム・トレーニング・メッセージに似たメッセージを暗号器バンク１７０の暗号器１７２に送らせる（ステップ４０３）ことによって安全ノードへの転送を開始する。これに応じて、暗号器１７２は、モデム応答信号をＣＰＥ１０１に送る（ステップ４０５）。暗号器１７２に関するトレーニングが進行中であることを示すために、ＣＰＥ１０１における何らかの表示、例えば、安全発呼ボタンに関係付けられた点滅する（安全）指示灯などを用いてもよい。

【００３０】初期のトレーニングが完了すると、安全な通信の確立の準備として周知のデータ通信プロトコルを用いて、キー交換シーケンスが開始される（ステップ４０７）。そのようなデータ通信プロトコルの１つが、ＡＮＳＩ規格Ｘ９．１７にも説明されているが、その他の多数の技術が当業者には周知である。必要であれば、暗号トレーニング中にコントローラ１５２によって発生される告知を被呼者で受信することもできる。ＣＰＥ１０１は、キーの交換が順調に完了すると直ちに安全指示灯が点滅を中止して光った状態を維持するように、構成してもよい。また、コントローラ１５２は、キー交換シーケンスの処理の完了を検出し、呼が安全モードに移行することを示す告知が発呼者に対して再生されるようにしてもよい。ひとたび安全モードになると、その呼の流れは、その呼の期間中、暗号器１７２およびコントローラ１５２を通り続ける（ステップ４１１）。

【００３１】発呼者が安全モードからクリア・モードに変更したい場合、例えばＣＰＥ１０１のクリア・ボタンを押す。この信号は、暗号器１７２で検出され（ステップ４１３）、これに応じて、暗号器がクリア・モードに移る。このクリア・モードへの転換は、呼をクリア・モードに転換する要求の合図をするべく、例えば暗号化されたデータには通常発生しないような独特のデータ・パタン（例えば、0011001100110011....のような繰り返しパタン）をＣＰＥ１０１が送る（ステップ４１５）ことによって実現される。暗号器１７２は、この独特なパタンを検出し、クリア・モードに切り替える要求をＣＰＥ１０１から受信したことを示すために、同じように

000111000111のような別の独特なパタンによって応答する。次に、ＣＰＥ１０１が、暗号器１７２によって返された信号に例えば0101010101010...などの第３の独特なパタンで応答して安全からクリアへのハンドシェイクを完了する（ステップ４１７）。このハンドシェイク処理は使用可能なプロトコルを説明するためのものであるが、その他の方法も当業者には明かである。その後、終了信号または切断信号が検出されるまで、呼は継続する（ステップ４１９）。

【００３２】発呼者および被呼者が異なる種類の暗号器／解読器を使用している場合、即ちＣＰＥ１０１およびＣＰＥ１０２が同じ暗号化アルゴリズムを使用していない環境において、両者の間で安全から安全の呼を行う時にも、本発明は使用することができる。この実施例では、暗号器バンク１７０において利用可能な２つの暗号器を用いることにより、安全ノード１５０が互換性のない暗号化／解読装置の間に暗号変換を与えている。

【００３３】ノード１５０における暗号変換によって安全な呼を発信するために使用される処理を図５に流れ図の形式で示す。この処理における最初のステップは、安全からクリアの呼に関連して既に説明したものと同じであり、従って、図２の処理を最初に行い、ＣＰＥ１０１とノード１５０との間の安全経路およびノード１５０からＣＰＥ１０２までのクリア経路を確立する。図６は、この種の呼に必然的に含まれるハードウェア要素を例示するもので、以下の説明の参考になる。

【００３４】呼経路の第２の区間（即ち、ノード１５０から被呼者の場所にあるＣＰＥ１０２まで）の通信もクリアであるより暗号化されるべきときには、通常、被呼者によってコントローラ１５２に合図が送られる（ステップ５０１）。（しかしながら、構造によっては、呼の両方の区間を暗号化するという判断がＣＰＥ１０１を使用する発呼者またはＣＰＥ１０２を使用する被呼者の一方によって合図されるものもある。）コントローラ１５２は、呼経路に第２の暗号器が必要であることを示す制御信号を検出すると、使用されている暗号器の種類を判定するためにＣＰＥ１０２に照会する（ステップ５０３）。この問い合わせにより、暗号器バンク１７０から適切な（第２の）暗号器を選択するために必要な情報がコントローラ１５２に与えられる。

【００３５】コントローラ１５２は、コントローラ１５２を通る経路が設定される第２の呼を確立するように信号を第２の出力ポート（図６におけるポート３１５）から交換機１５１に送る（ステップ５０５）。多くのＰＢＸ交換機は現在のところ出接続呼の「転送」も「ブリッジ」もできず、入接続呼の転送またはブリッジしかできないので、この構造を使用する。また、この構造を用いるのは、呼経路のうち通信がクリアな部分にコントローラ１５２を残すためでもある。このことは以下において十分説明する。尚、図６において、コントローラ１５２への第２の呼はポート３１５に端を発し、交換機１５１の入力ポート６０１に至り、この交換機により、その出力ポート６０２を介して異なる入力ポート６１１にてコントローラ１５２に接続される。

【００３６】コントローラ１５２により、ＣＰＥ１０２における発呼者によって使用されている特定の暗号器の種類に関係付けられたハント・グループを特定する情報をデータベースの参照を用いて決定する（ステップ５０７）。次に、コントローラ１５２は、コントローラ１５２のポート６１２から出力され交換機１５１の入力ポート６０３に加えられるハント・グループに関する番号への呼を開始し、適切な暗号器が使用できると交換機が判断した場合（ステップ５０９）、交換機が暗号器バンク１７０における適切な種類の次に利用可能な暗号器（例えば、図６における暗号器１７４）に呼を接続する（ステップ５１３）ようにさせる。利用できないと判断した場合、ステップ５１１において終了メッセージを再生する。

【００３７】暗号器１７４は、暗号器１７２と同様に、その出力が交換機における回線側の終端（ポート６０５）に接続されるように構成されている。しかし、この例では、暗号器１７４も、交換機１５１の出力ポート６０６からコントローラ１５２の異なる入力ポート（ポート６１３）への間の交換機１５１における接続を実施するために必要な信号が暗号器１７４が動作状態になった時に常に生成されるように、構成されている。これは、暗号器バンク１７０のいくつかの暗号器を交換機１５１における「仮想的な直通回線」接続（暗号器がその入力ポートで呼を受信することにより動作状態になったときコントローラ１５２の利用可能なポートに自動的につながる）に接続されるように調整することによって、実現される。仮想的な直通回線は、交換機１５１の回線側の１つ以上の終端のオフ・フック状態を検出するように交換器１５１をプログラムし、オフ・フック状態の検出時にコントローラ１５２またはＣＰＥからの合図をさらに必要とすることなく呼を自動的にプログラムされた目的点に経路設定することによって実施される。

【００３８】コントローラ１５２が「直通回線」の呼をポート６１３で受信すると、その入力ポート３１３間の接続を出力ポート３１４から出力ポート３１５へと切り替える（ステップ５１７）ようにコントローラ１５２を調整する。同時に、ポート６１３および３１４がコントローラ１５２の内部で接続され、ポート６０２および６０４が交換機１５１の内部で接続される。この状態における呼経路を図７に示す。次の点に注目する必要がある。

【００３９】（ａ）呼経路に２つの暗号器１７２および１７４があり、第１の暗号器はＣＰＥ１０１から受信される暗号化されたメッセージを安全な形式からクリアな形式に変換するのに適した型のものであり、第２の暗号

器はＣＰＥ１０２から受信される暗号化されたメッセージを安全な形式からクリアな形式に変換するのに適した型のものである。

【００４０】（ｂ）暗号器「１７２および１７４の間の呼経路のクリアな部分にコントローラ１５２が残る。従って、必要ならば、回線の両端の当事者によってコントローラ１５２に信号を送ることができる。

【００４１】図５の処理は、制御信号または終了信号を求めて呼を監視する（ステップ５１９）ことにより完了する。既に説明した実施例の場合のように、呼の終了は、ＣＰＥ１０１またはＣＰＥ１０２の何れかがハンドセット（送受器）を置いたときに通常どおり実現される。この場合、切断信号が交換機１５１またはコントローラ１５２によって検出され、接続が取り払われる。

【００４２】図８において、ＣＰＥ１０１は安全な音声端末であり、通常の可聴周波入力（マイクロフォン）および可聴周波出力（拡声器）を備えたハンドセット８００はハンドセット・インタフェース８０１に接続され、線８０２でアナログ信号（２００から３０００Ｈｚ）を送受信する。外に向かう信号（ＣＰＥ１０１で生成され交換機１０７を介して被呼者に送られる信号）については、インタフェース８０１の出力はアナログ／デジタル変換器８０３に接続され、そこで、可聴周波帯域信号が例えば５６Ｋbpsの標本化され且つ量子化されたパルス符号変調（ＰＣＭ）デジタル信号へとデジタル化される。このようにするのは、ＣＰＥ１０１ではデジタル処理の方が好ましいからである。

【００４３】アナログ／デジタル変換器８０３の出力は、音声符号器／復号器（音声コーデック）８０５に加えられる。コーデック８０５は、受信したビット・ストリームをデジタル・ワード・ストリームに一般に２４００bpsで圧縮する。圧縮の一種として、ＡＴ＆Ｔから入手可能なＳＴＵ III安全音声端末に見られる種類の符号励起線形予測（ＣＥＬＰ）符号器／復号器がある。この圧縮符号化を行うのは、暗号作成モジュール８０７において実行される暗号化／暗号解読を容易にするためである。このモジュールは、記憶されている暗号キーを用いてクリアなデータと安全なデータとの間で周知の翻訳を行うように構成される。暗号化の本質は、暗号キーにアクセスする資格を有する利用者のみに安全なデータを解読することを許し元の情報を再生できるようにすることである。暗号作成モジュールの一例は、連邦情報処理規格（ＦＩＰＳ）１４０－１「暗号作成モジュールに対する安全条件（Security Requirements for Cryptographic Modules）」の１９９０年７月付けの草案に説明がある。

【００４４】暗号作成モジュール８０７の出力は、モデム８０９へ、そしてＤ／ＡおよびＡ／Ｄ変換器８１１へと加えられるが、両者は、共に信号路に挿入され、暗号作成モジュール８０７から出力された２４００bpsのデジタル信号をアナログ電話回線上の伝送に適したアナログ・モデム・トーンのシーケンスへと変換することを目的とする。モデム８０９自体が、２４００bpsのモデム出力を例えば５６ｋbps（これは、デジタル電話回線への応用に適している）のデジタル・ビット・ストリームへと変換する。このビット・ストリームは、可聴周波トーンを表す。信号が暗号化（スクランブル）されているので、トーンは、資格のない聴取者の場合、元の音声メッセージに含まれている情報を判断することができないようにスクランブルされる。

【００４５】ＣＰＥ１０１は一般にＬＥＣ交換機１０７への通常のアナログ加入者アクセス・ループを通して電気通信網に接続されるので、モデム８０９の出力は、電話回線インタフェース８１３を介して前記のループに加えられる前にＤ／ＡおよびＡ／Ｄ変換器８１１においてデジタル形式（５６ｋbps）から元のアナログ形式に変換される。デジタル・アクセスが提供されている場合には、Ｄ／ＡおよびＡ／Ｄ変換器８１１、インタフェース８１３、またはこれらの両方とも必要でないこともある。

【００４６】中に向かう信号（安全ノードで生成され、交換機１０７を介してＣＰＥ１０１に向かう信号）についても同様の変換が行われる。具体的には、スクランブルされた可聴周波トーンを表すアナログ入力が、インタフェース８１３を介して受信され、Ｄ／ＡおよびＡ／Ｄ変換器８１１でデジタル形式に変換される。一連のアナログ・トーンを表すＰＣＭのビット・ストリームは、モデム８０９において（例えば）２４００bpsのビット・ストリームに変換され、暗号作成／解読モジュール８０７で解読され、コーデック８０５において記号がデジタル・ビット・ストリームに変換され、元のアナログ信号を表す。デジタル・ビット・ストリームは、変換器８０３において理解できるアナログ形式に変換されてから、最終的にインタフェース８０１を介してハンドセット８００に加えられる。

【００４７】図８に示したＣＰＥ構造は、前面パネルインタフェース回路８２０も備え、この回路によって、クリア・ボタン８２１、安全ボタン８２４、およびキーパッドまたはその他の入力装置８２２からの入力を受信し、さらにこの回路は、ＬＥＤ、ＬＣＤまたは類似の表示装置によって与えられるような視覚的表示を動作させるように構成される。インタフェース８２０で受信される入力は、メモリ８４０に記憶されたプログラムの制御下で動作するマイクロプロセッサ８３０において局部的に処理される。また、マイクロプロセッサ８３０は、Ｄ／ＡおよびＡ／Ｄ変換器８０３、８１１、コーデック８０５、モデム８０９、さらに大抵の場合暗号作成／解読モジュール８０７の動作と相互に作用しあい、それらの動作を制御し、かつそれと協調するようにプログラムされる。この後者の相互作用には、キーの記憶／検索、お

よびその他の暗号関連の機能が含まれる。

【００４８】図８では、暗号化／暗号解読の要素および関係する信号の変換が電話局に対して内部的に行われるＣＰＥを考察するが、構造によっては、通常の端末に先に説明したような機能を与えるために、通常の端末に「安全電話装置（ＳＴＤ）」として周知の外部装置を取り付ける方が好ましいこともある。この構造では、ＳＴＤはハンドセットと電話ベースとの間の利用者の電話機に取り付けられる。別個のＡＣトランスによりＳＴＤに電力を供給する。ＳＴＤは、多くの種類の電子的、モジュラー式、かつ押しボタン式の業務用および家庭用の電話機と互換性がある方が好ましい。必要に応じて、利用者は、ＳＴＤ上の表示装置およびソフトウェアで定義されたスイッチによってＳＴＤの仕様を変更することができる。このような表示装置によって、安全またはクリアのモードの確認、および通信が無資格者によって変更されていないことを保証する視覚的信号を利用者に与えられる。ＳＴＤは携帯できるほど十分に小型かつ軽量にすることができるので、都合良くいろいろな場所（例えば、仕事場、自宅、旅行先など）に持ち運ぶことができる。

【００４９】図９において、コーデック８０５、暗号作成／解読モジュール８０７およびモデム８０９などの多くの要素は、図８に関連して説明したものと同じである。しかしながら、各暗号器は、一般にＰＢＸ、即ち交換器、特に図１のデジタル・スイッチ１５１からの入力を受信し、かつそれに出力を供給する。この理由から、アナログからデジタルへの変換は必要ないので、Ｄ／ＡおよびＡ／Ｄ変換器８０３および８１１が無い。さらに、ハンドセット・インタフェース８０１および電話回線インタフェース８１３によって行われる機能は、１対のＰＢＸインタフェース回路９０１、９１３によって実行される。

【００５０】また、図９の暗号器には、図８の前面パネルインタフェース８２０の代わりに信号インタフェース９２０が含まれる。これは、暗号器が都合良く電気通信網の中に位置し、かつ発呼者および被呼者によってコントローラ１５２の機能を用いて信号が送られるためである。

【００５１】先に説明した呼の発信シーケンスは説明のためのものであり、当業者であれば電気通信網の他の構成要素に付加的な知能を組み込む場合に利用可能な種々の代替的な処理が分かるであろう。一例をあげる。図１のデータベース１２０は、選択された発呼者および被呼者の番号に関する付加的な情報を取り出すことができ、交換機１１０および（または）１２５は、信号網１１５を介して受信される情報に応じて対話的なシナリオを実行できるものと仮定する。この実施例において、発呼者が安全ノード１５０のアクセス番号をダイヤルすると、その呼は、特殊な処理を必要とするものとデータベース１２０によって認識される。発呼者は、例えばその呼の種類、即ちその呼が安全からクリアの呼か、クリアから安全の呼か、または安全から安全の呼かを明確にするように交換機１１０によってプロンプトが出される。安全からクリアの呼の場合、発呼者は、ＣＰＥ１０１上のタッチトーン・パッドを用いて利用者のＩＤ番号を入力するようにプロンプトが与えられる。交換機１１０は、データベースと連携して、利用者のＩＤ番号の正統性を確認しようとする。利用者のＩＤが確認できない場合、利用者は、この状態の通知を受け、正当な利用者ＩＤ番号を入力し直すように求められる。試行を２回行った後も、利用者のＩＤ番号の正統性が確認できない場合、利用者は、問題があるとの通知を受け、さらに支援を受けるため別の電話番号でサポート・センターに電話するように求められて、呼が取り除かれる。このように、図２のステップ２０３、２０５、および２０７の部分は、ノード１５０の外側で実行してもよい。

【００５２】図１のシステムを用いて安全からクリアの呼を確立する代案の過程を図１０の流れ図および図１１～１５のハードウェア図で説明する。（クリアから安全の呼、および安全から安全の呼に対しても同様の過程をたどる。）この過程は、いくつかの重要な点において前記のものとは異なる。第１に、発呼者および被呼者との間で端から端までの接続が確立されてから、呼経路に暗号器が挿入される。第２に、暗号化が始まると、コントローラ１５２が呼経路から削除される。第３に、当事者の何れかが安全な通信の開始を希望すると、暗号器の「型」の情報がノード１５０に自動的に与えられる。

【００５３】呼の受信に応じて処理が開始し（ステップ１００１）、これに基づいて、交換機コントローラ１５２は、呼の完成に必要なログイン、パスワード、および被呼者の番号の情報を求めて発呼者にプロンプトを出す（ステップ１００３）。暗号器の「型」の情報は、この時点では与えられない。情報が収集され（ステップ１００５）、データベース１５４に記憶される。発呼者が有資格利用者である場合（ステップ１００７）、コントローラ１５２は、（ＣＰＥ１０１からの）入接続呼を保留し（ステップ１０１５）、ステップ２１７においてＣＰＥ１０２への呼を開始するために先にデータベース１５４に記憶された被呼者の情報を交換機１５１に送る。図２の処理の場合のように、この呼の経路は、コントローラ１５２から線１６８を介して交換機１５１へ、交換機１５１からトランク１６３を介して交換機１２５へ、さらに電気通信網を通ってＣＰＥ１０２へと至る。発呼者が資格ありと認められた場合、課金および請求処理が開始され（ステップ１０１１および１０１３）、発呼者が資格ありと認められない場合、終了の告知が再生される（ステップ１００９）。

【００５４】被呼者が応答すると、コントローラ１５２は、コントローラ１５２への呼をコントローラ１５２か

らの呼にブリッジするように交換機１５１に信号で合図する。これにより、両当事者の間にクリアな通信路が確立され、その通信路にコントローラ１５２の１つの「出現」が一時的に残されるので、そのコントローラ１５２により、何れかの当事者が呼をクリア・モードから暗号化モードに移すように希望していることを示す制御信号の発生を求めて呼を引き続き「監視する」（ステップ１０２１）ことができる。

【００５５】ステップ１０２３において、何れかの当事者がその当事者のＣＰＥとノード１５０との間の伝送路の部分を伝送される情報の暗号化を望んでいることを示す「安全伝送開始」の信号をコントローラ１５２に送った判断される場合、そのＣＰＥで使用されている暗号器の種類の判定が行われる（ステップ１０２５）。この判定は、コントローラ１５２によって「自動的に」行われ、このときコントローラ１５２は、「安全伝送開始」信号と一緒に送られる暗号の型を表す符号を認識する。「安全伝送開始」信号が検出されるまで、ステップ１０２１が繰り返される。

【００５６】トレーニング・メッセージは、発呼者によって使用されている暗号化装置の型を指定するＤＴＭＦトーンまたはその他の信号情報を含む。また、交換機１５１にある付属交換機アプリケーション・インタフェース（ＡＳＡＩ）により、呼の設定中にＣＰＥ１０１において発生されたＤＴＭＦトーンを認識することができる。この場合、暗号器の型だけでなく、その型の暗号器に関係付けられたハント・グループ番号（複数可）も自動的に決定して、コントローラ１５２に送ることができる。

【００５７】ステップ１０２５には、適切な暗号器に対する「ハント・グループ」の決定も含まれる。具体的には、コントローラ１５２が「安全伝送開始」信号を発したＣＰＥで使用されている暗号器の型を判定したときに、データベース１５４において参照動作を行って暗号バンク１７０内部の適切な暗号器に関係付けられたハント・グループの指定を確認する。次に、ステップ１０２７において、コントローラ１５２が、交換機１５１に信号で合図を送り、一方の当事者（即ち、「暗号化開始信号」を発生しなかった方の当事者）を保留し、かつ選択された暗号器の種類に関係付けられたハント・グループに呼を発するようにさせる。そのハント・グループが呼び出されると、次に利用可能な適切な種類の暗号器（例えば、図１の暗号器１７２）が交換機１５１によって選択される。しかしながら、選択された種類の暗号器が利用できない場合（ステップ１０２９）、処理は終了する（ステップ１００９）。

【００５８】暗号器１７２のトレーニング（ステップ１０３１）は、図５に関連して既に説明した過程と同じ過程をたどるが、これが完了すると、ステップ１０３３において、トレーニング期間中に他方の当事者（即ち、ステップ１０２３の暗号化要求に関係していない当事者）が通信路の残りの部分で送られるメッセージの暗号化の開始要求を信号で送ったかどうかについて判断を行う。送っていない場合、ステップ１０２７において保留された呼およびコントローラ１５２から暗号器１７２への呼がステップ１０３５においてブリッジされる。この時点で、交換機１５１に適切な制御信号を送ることによって通信路からコントローラ１５２を取り除くことができ、これによって交換機の内部にブリッジ接続が確立される。しかしながら、通信路におけるコントローラ１５２によって暗号器のトレーニングが完了したのであるから、通信路からコントローラ１５２を除去することが、ＣＰＥ１０１および１０２ならびに暗号器１７２および１７４が暗号化通信を継続する能力を妨げないことが重要である。これについては、コントローラ１５２により通信路に無視できる程度の遅延および周波数歪しか挿入されないことを保証することによって、対処することができる。

【００５９】他方の当事者が暗号開始の要求信号を送った場合、その当事者の暗号器の種類に関してステップ１０２５～１０３１が繰り返される。このようにして、安全から安全の呼が完成する。

【００６０】図１１～１５のハードウェア図によって図１０に示した処理を説明する。図１１は、ステップ１０１９が完了した後のＣＰＥ１０１および１０２、交換機１５１およびコントローラ１５２の配置を表す。コントローラ１５２は発呼者と被呼者との間に存在するクリアな通信路に挿入されている点に注目する必要がある。

【００６１】図１２は、ステップ１０３１が完了した後の同じハードウェア構成要素の配置を示す。処理のこの点において、暗号器１７２は、ＣＰＥ１０１の中の暗号化モジュールについてトレーニング中であり、同時にＣＰＥ１０２の被呼者は、保留状態にあり、一般に、他方の当事者とトレーニングが進行中であることを示す告知をコントローラ１５２の音声応答ユニット１５３から受信している状態である。

【００６２】図１３において、安全からクリアの呼について図１０の処理が完了する。ハードウェアの配置は、通信路にコントローラ１５２がないことを除けば、図３に示したものと類似している。

【００６３】図１４は、ステップ１０３３において他方の当事者が暗号化を開始するときに、安全から安全の呼に伴う付加的な要素を示す。同図において、被呼者のＣＰＥ１０２にある暗号化モジュールは、第２の暗号器、即ち暗号器１７４についてトレーニング中である。トレーニング処理が終了すると、ハードウェアの配置は、図１５に示したようになる。この配置は、コントローラ１５２が通信路にないことを除けば、図７に示したものと類似したものとなる。

【００６４】以上の説明は、本発明の一実施例に関する

もので、この技術分野の当業者であれば、本発明の種々の変形例が考えられるが、それらはいずれも本発明の技術的範囲に包含される。いくつかの例を示す。

【００６５】不正およびその他の悪用を防ぐために、安全ノード１５０にアクセスするための呼の発呼者あたりの試行回数（ＡＮＩを監視することにより判定する）を追跡するように安全ノードを構成してもよい。所定の期間内に所定の回数の試行が行われた後、安全ノードは、その発呼者（ＡＮＩ）がそれ以上そのノードにアクセスしようとするのを自動的に阻止する。安全な番号指定も提供することができる。これにより、被呼者の番号を入力する前にＳＴＤまたはＣＰＥから安全ノードへの呼の安全が確保されるので、被呼者の番号および（または）発呼者のダイヤル・パタンが盗聴者に知られることがない。

【００６６】本発明は、既に利用可能な種々のサービスのみならず将来提供する予定の新たな多くのサービスとの関連においても使用することができる。例えば、安全な音声およびファクシミリの記憶および検索では、クリアから安全の呼をサポートし、呼び出し時に応答がないか話中の場合の入接続メッセージを安全なメールボックスに渡せるようにすると、そのメッセージは被呼者により後にアクセスできるように暗号化された形式で記憶される。これにより、暗号化されたメッセージが資格のある当事者によって取り出されるまで、そのメッセージを安全な場所に保管することができる。発呼者は、そのメッセージが意図する受信者に届くまで、情報の安全が保証される。

【００６７】前記の説明の部分は音声の呼について述べたが、本発明は、あらゆる種類のデータの安全な通信にも関連付けて同様に利用することができる。例えば、本発明は、ＰＣ間の通信およびＰＣとメインフレーム・コンピュータとの間の通信の保護に対しては理想的である。この用途には、電話装置と電話回線との間のＳＴＤインタフェースを適切に変更するだけでよく、これは普通の技術で容易に実現できる。同様に、安全なファクシミリを用いて、ファクシミリ装置間の通信、ならびにファクシミリの記憶および転送サービスを保護することができる。ファクシミリ受信（ファクシミリが誰に配信されたか）の正真性の証明を与えることもできる。

【００６８】通話の課金については、種々の解決方法が可能である。例えば、発信側および受信側のＡＮＩおよび各利用者のＩＤ番号に関係付けられた通話時間の情報を安全ノード１５０が捕捉するように安全ノードを構成してもよい。この情報を主課金番号と共に課金評価／書式化システム１８７に渡し、その加入者の発信通話表に基づいて処理して、その加入者の請求額に加える。呼は、発信地と安全ノードと受信地との間ではなく発信地と受信地との間の呼の流れに基づいて評価される。従って、安全ノード１５０との間の呼のやりとりの費用は、

一般に暗号化／暗号解読の特別料金の一部となり、加入者の請求書に項目としては現れないことになる。課金は、被呼者から安全ノード１５０に応答指示が与えられた時に開始される。加入者が発信した呼（即ち、安全からクリアの呼、安全から安全の呼）に対しては異なる課金構造を用いることができる。この場合の通話の費用は、発信した加入者の請求額に適用することができる。これに対し、クリアから安全の呼の場合は、（コレクト・コールにように）受信側の加入者が通話費用の責任を負うことになる。

【００６９】最後に、以上の説明では交換機１５１およびコントローラ１５２を別個の装置として述べたが、呼の監視、音声プロンプトの発生および応答の収集、情報の記憶、蓄積プログラムの制御下での接続、および種々の関係付けられた機能の実行が可能な単一の「インテリジェント交換機」を電気通信網の中に配置して代用することができる。

【００７０】

【発明の効果】以上述べたように、本発明によれば、呼の当事者の双方がハンドシェイク・プロトコルおよび暗号アルゴリズムの異なる安全装置を有する場合も、また当事者の一方のみが安全装置を有する場合も、比較的安全な通信を行うことができる。

【図面の簡単な説明】

【図１】本発明によって構成された安全ノードを例示するブロック図である。

【図２】「安全からクリア」の通信経路、即ち発呼者（ＣＰＥ１０１）と安全ノードとの間の安全な接続、および安全なノードと被呼者（ＣＰＥ１０２）との間のクリアな接続を設定するために図１のコントローラ１５２において実行されるステップを例示する流れ図である。

【図３】安全からクリアの通信を開始する過程を説明し、そのような呼またはメッセージに対する図１の構成要素の幾つかを通る経路を例示するために役立つハードウェア流れ図である。

【図４】暗号器バンク１７０およびＣＰＥ１０１および１０２の暗号器において実行されるハンドシェイク・ステップを例示する流れ図である。

【図５】「安全から安全」の通信を設定するためにコントローラ１５２において実行されるステップを例示する流れ図である。

【図６】安全から安全の通信を開始するための設定過程に伴う付加的な要素を示す図３と同様の図である。

【図７】図６の構造を用いて安全から安全の通信が確立された後の経路を示す図である。

【図８】図１のＣＰＥ１０１のような典型的な加入者の構内装置の要素を示すブロック図である。

【図９】暗号器バンクの内部の暗号器１７２および１７４などの典型的な暗号器の要素を示すブロック図である。

25

【図１０】安全なノード１５０を用いて安全からクリア、クリアから安全、安全から安全の呼を完成させるための代案の過程を示すブロック図である。

【図１１】図１０の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図１２】図１０の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図１３】図１０の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図１４】図１０の過程における種々のステップの期間中のハードウェア構造を示す図である。

【図１５】図１０の過程における種々のステップの期間中のハードウェア構造を示す図である。

【符号の説明】

１０１、１０２
加入者構内装置（ＣＰＥ）

１０７、１１２
市内交換機

１０８、１１１
市内交換キャリア（ＬＥＣ）局

１１０　相互交換キャリア交換機

26

１１５　共通チャネル信号（ＣＣＳ）網

１１６　信号転送点（ＳＴＰ＝signal transfer point)

１２０　着信ワッツ(InWATS)データベース（ＩＤＢ）

１５０　安全ノード

１５１　交換機（SWITCH）

１５２　交換機コントローラ（SWITCH CONTROLLER, CONTROLLERまたはCONT）

１５３　音声応答ユニット（ＶＲＵ）

１５４　データベース（ＤＢ）

１５６　交換通信網

１６０　トランク

１６１　線群

１７０　暗号器バンク

１７２、１７４
暗号器／解読器

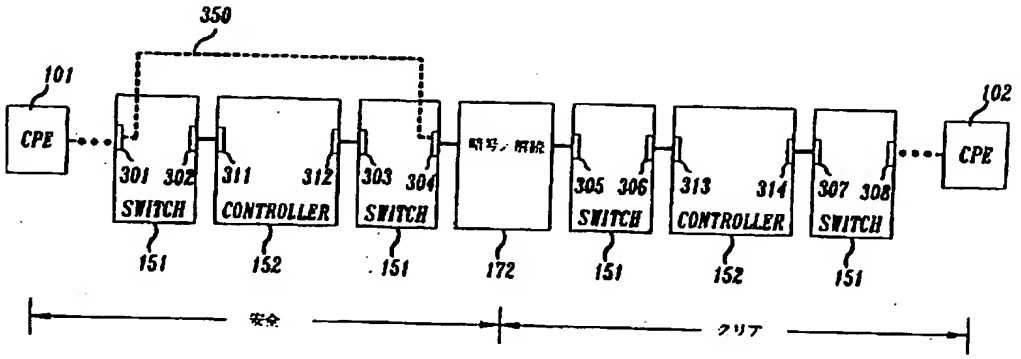
１８０　通話カード・データベース

１８５　記録／課金プロセッサ

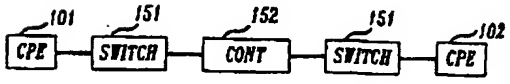
１８７　課金評価／書式化システム

１９１、１９２
安全電話装置（ＳＴＤ）

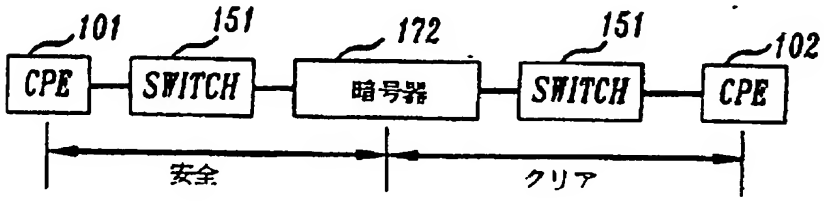
【図３】



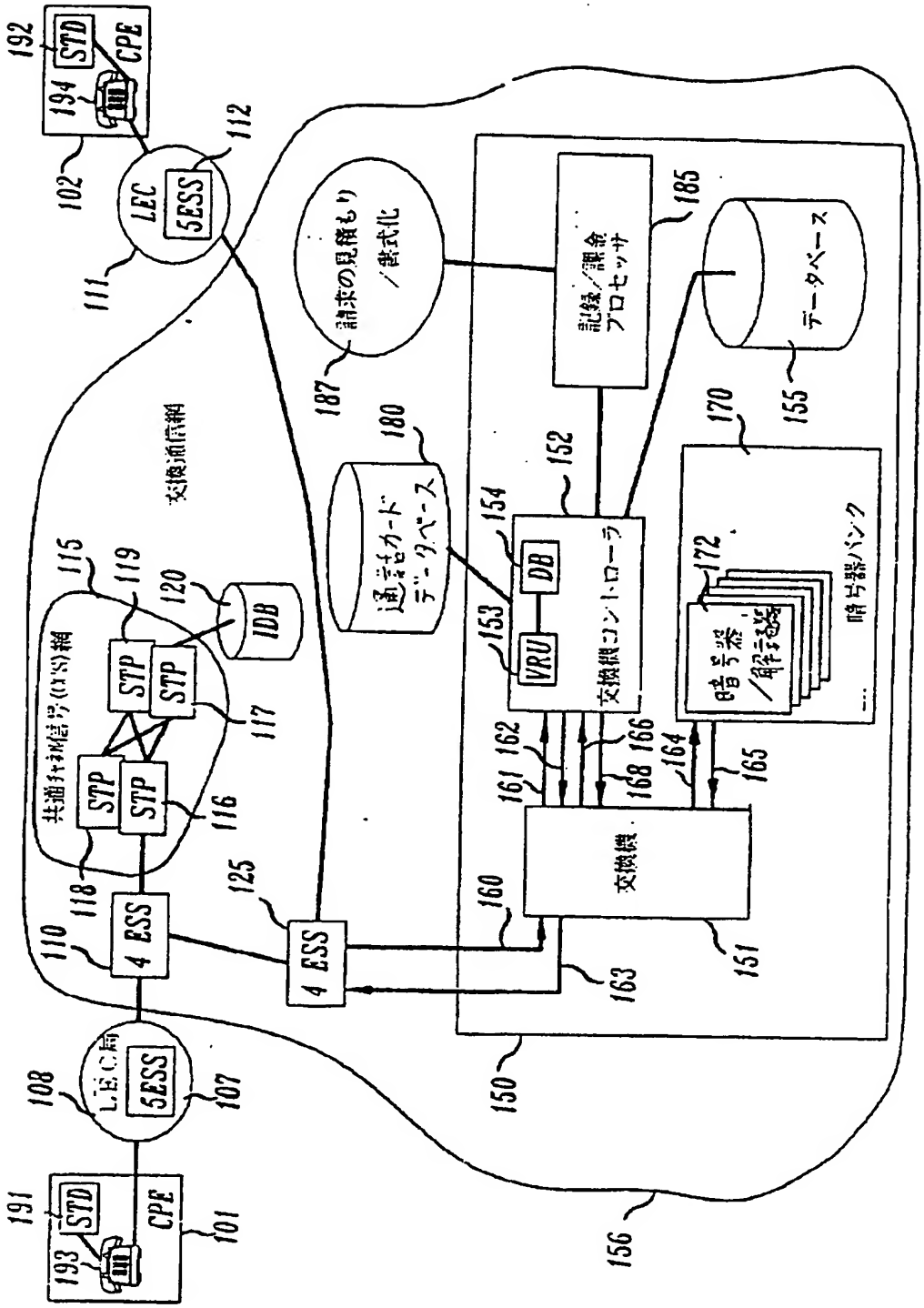
【図１１】



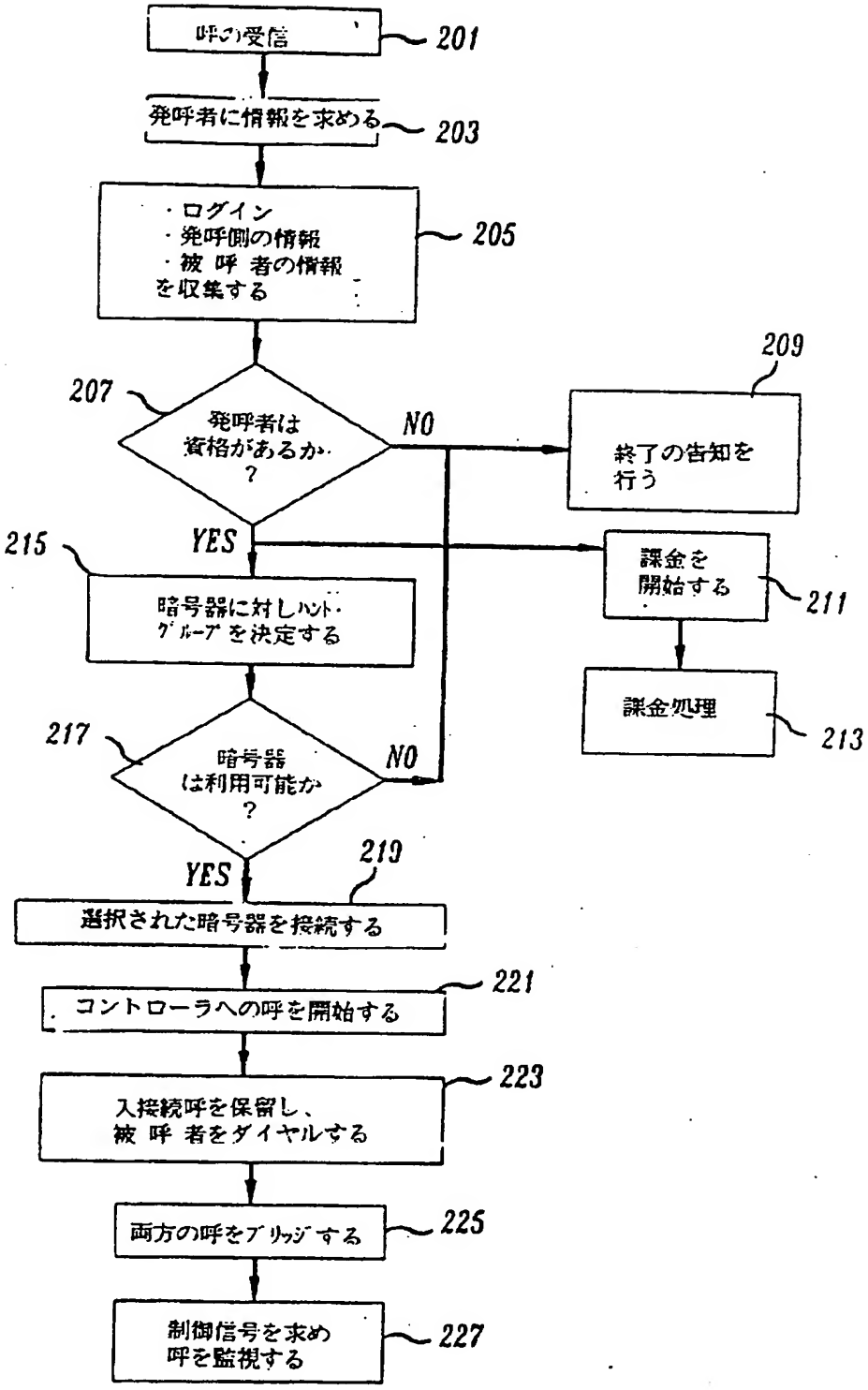
【図１３】



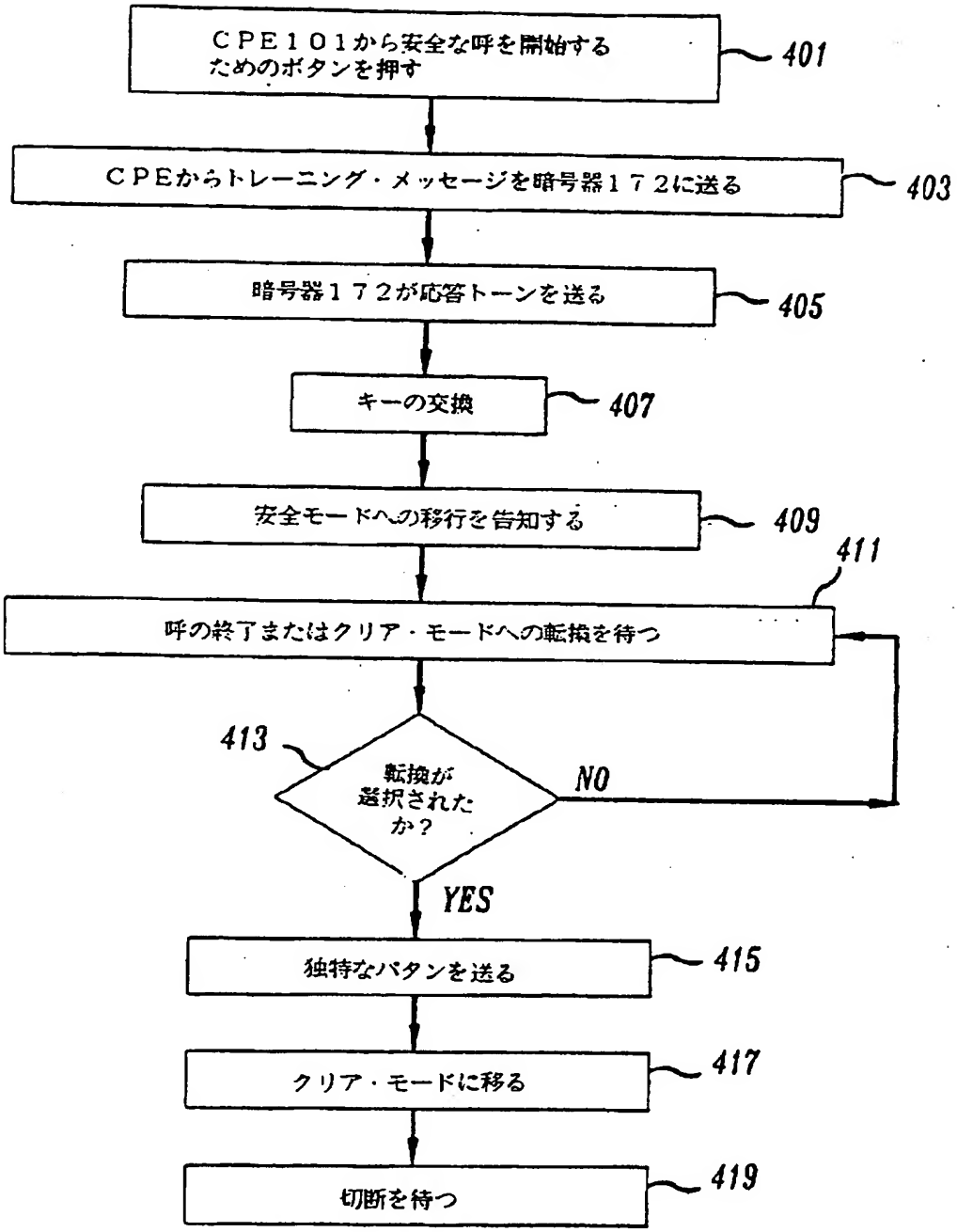
【図1】


192
STD
194
CPE
102
LEC
5ESS
112
111
交換通信網
請求の見積もり／書式化
187
180
通話カードデータベース
154
152
DB
153
VRU
交換機コントローラ
記録／課金プロセッサ
185
データベース
155
170
172
暗号器／解読器
暗号鍵バンク
115
119
120
IDB
共通線信号(CCS)網
STP
117
116
118
110
4 ESS
125
160
交換機
151
163
161
162
166
168
164
165
150
156
108
LEC局
5ESS
107
191
193
101

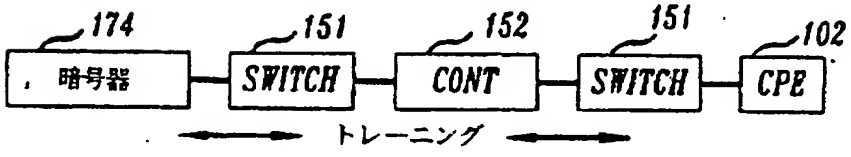
【図２】


呼の受信
201
発呼者に情報を求める
203
・ログイン
・発呼側の情報
・被呼者の情報
を収集する
205
207
発呼者は資格があるか？
NO
209
終了の告知を行う
YES
215
暗号器に対しハント・グループを決定する
課金を開始する
211
課金処理
213
217
暗号器は利用可能か？
NO
YES
219
選択された暗号器を接続する
221
コントローラへの呼を開始する
223
入接続呼を保留し、被呼者をダイヤルする
225
両方の呼をブリッジする
227
制御信号を求め呼を監視する

【図４】


ＣＰＥ１０１から安全な呼を開始するためのボタンを押す
401
ＣＰＥからトレーニング・メッセージを暗号器１７２に送る
403
暗号器１７２が応答トーンを送る
405
キーの交換
407
安全モードへの移行を告知する
409
411
呼の終了またはクリア・モードへの転換を待つ
413
転換が選択されたか？
NO
YES
独特なパタンを送る
415
クリア・モードに移る
417
切断を待つ
419

【図１４】


174
暗号器
151
SWITCH
152
CONT
151
SWITCH
102
CPE
トレーニング

【図５】

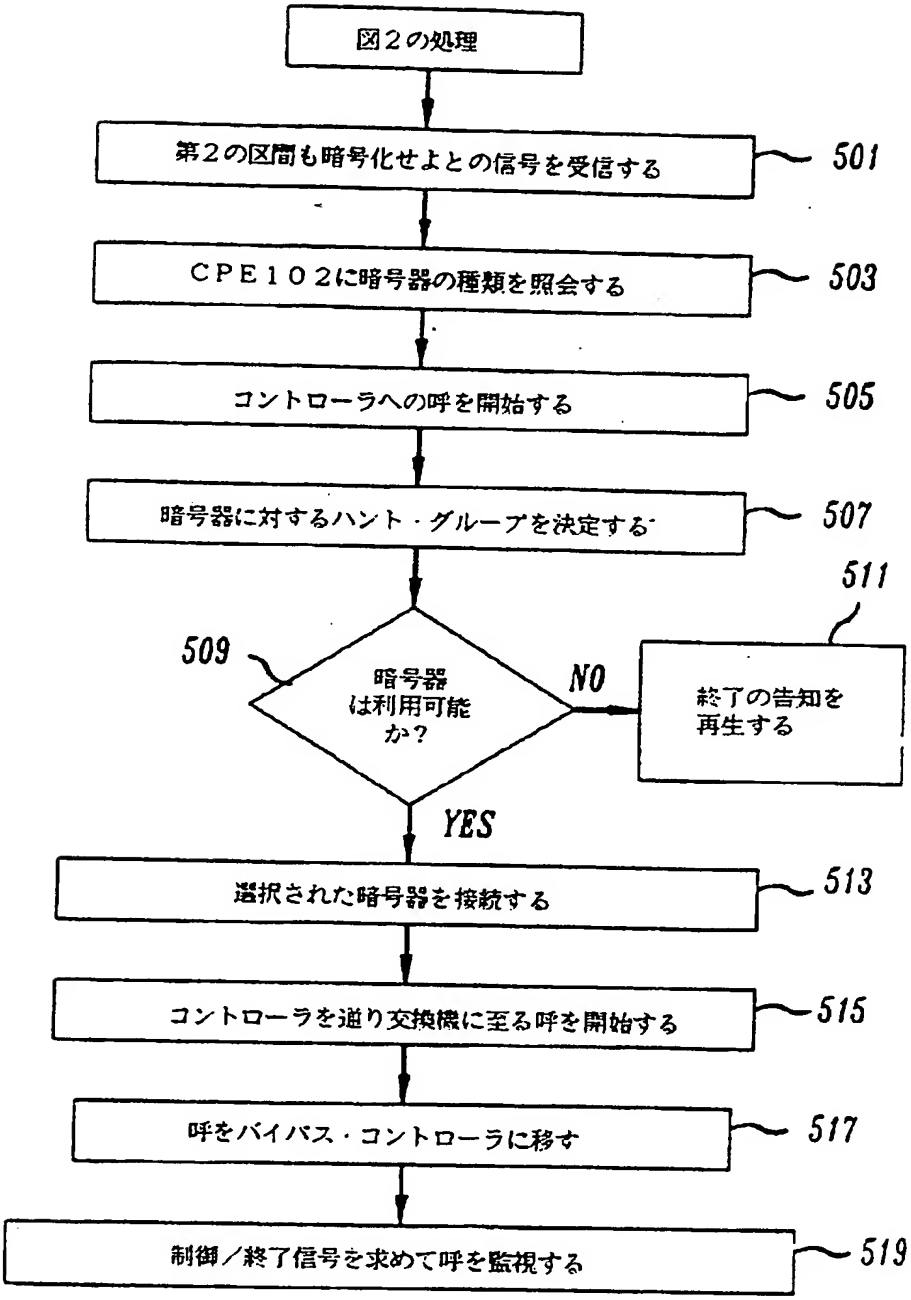
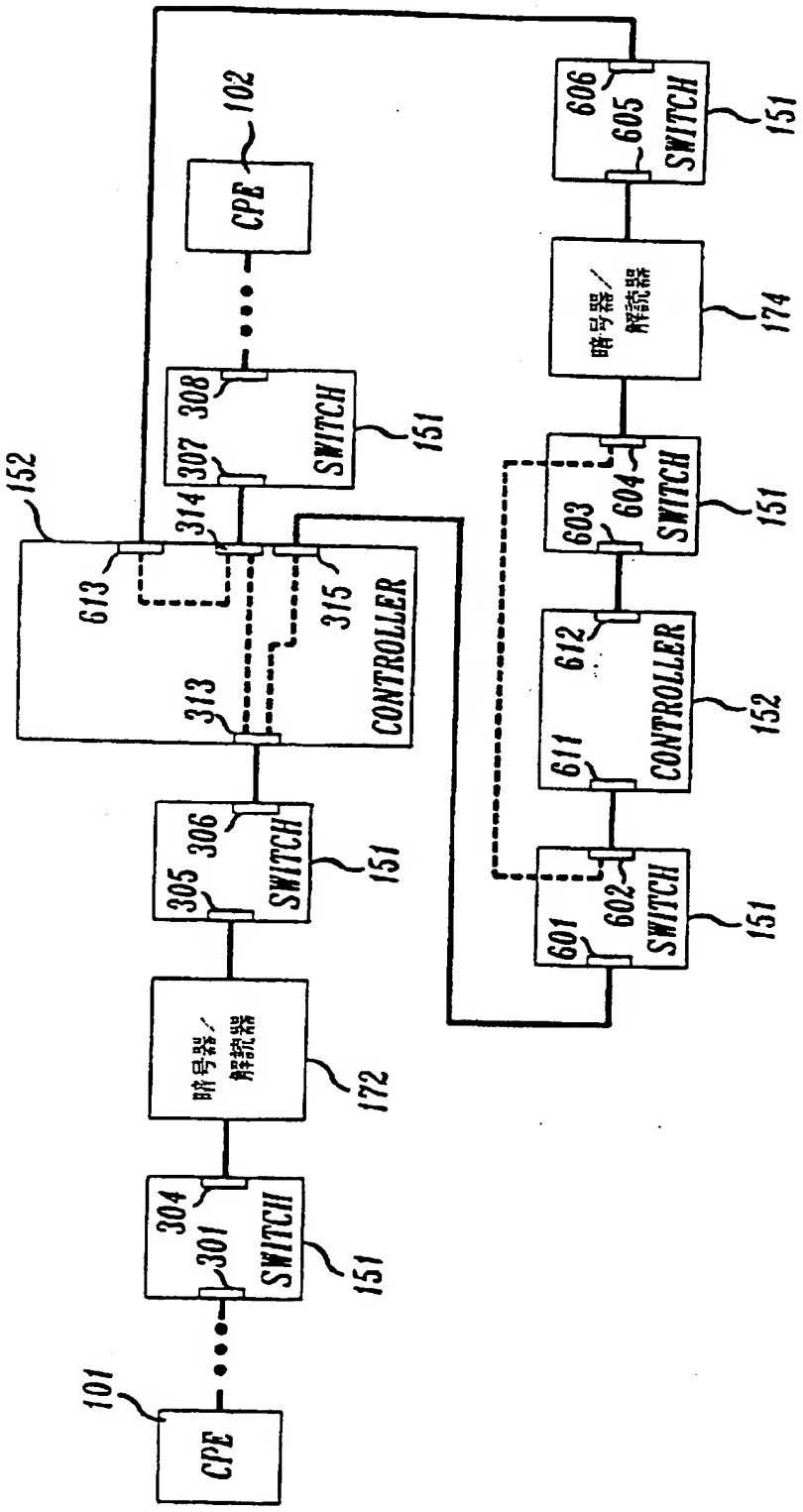
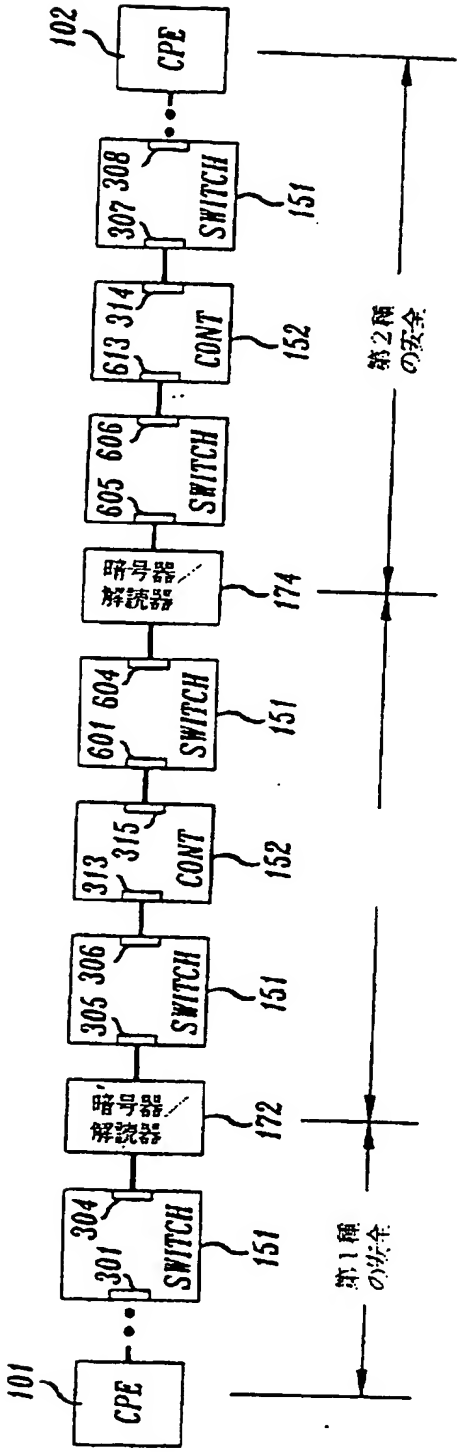


図２の処理
第２の区間も暗号化せよとの信号を受信する
501
ＣＰＥ１０２に暗号器の種類を照会する
503
コントローラへの呼を開始する
505
暗号器に対するハント・グループを決定する
507
509
暗号器は利用可能か？
NO
511
終了の告知を再生する
YES
選択された暗号器を接続する
513
コントローラを通り交換機に至る呼を開始する
515
呼をバイパス・コントローラに移す
517
制御／終了信号を求めて呼を監視する
519

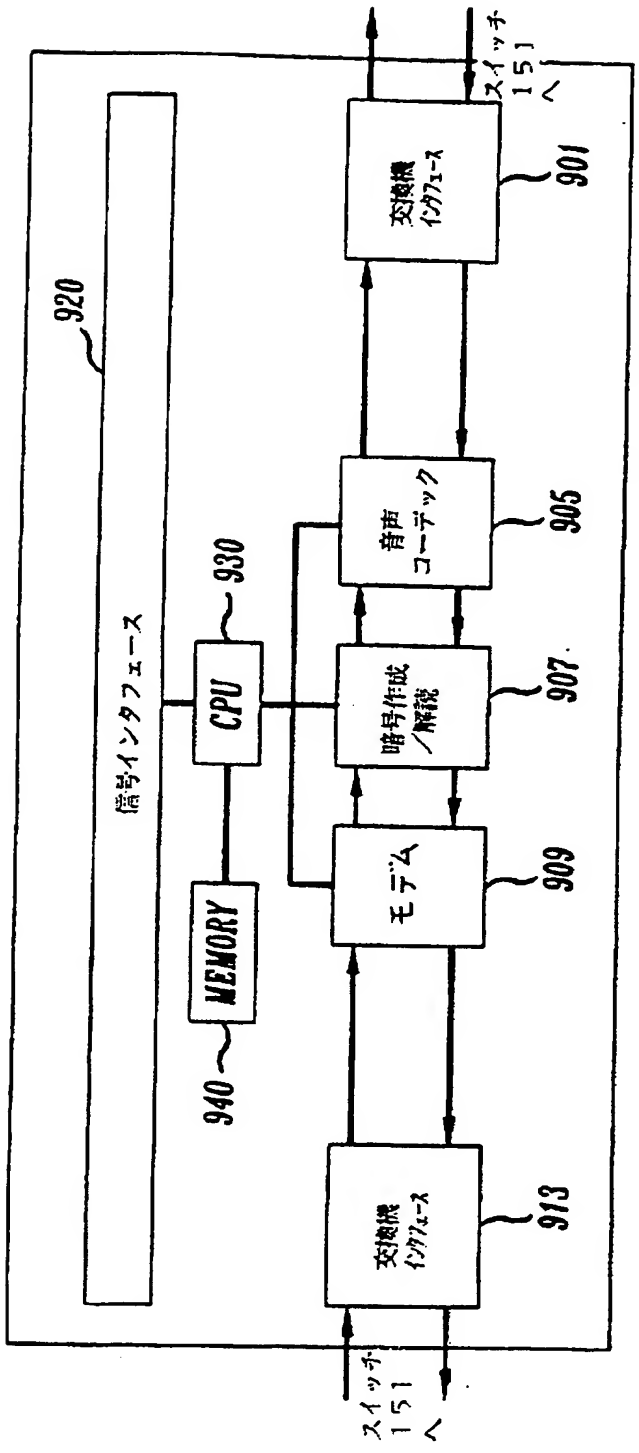
【図６】


CPE
102
308
307
SWITCH
151
152
314
613
315
CONTROLLER
313
306
305
SWITCH
151
暗号器／解読器
172
304
301
SWITCH
151
101
CPE
606
605
SWITCH
151
暗号器／解読器
174
603
604
SWITCH
151
612
611
CONTROLLER
152
601
602
SWITCH
151

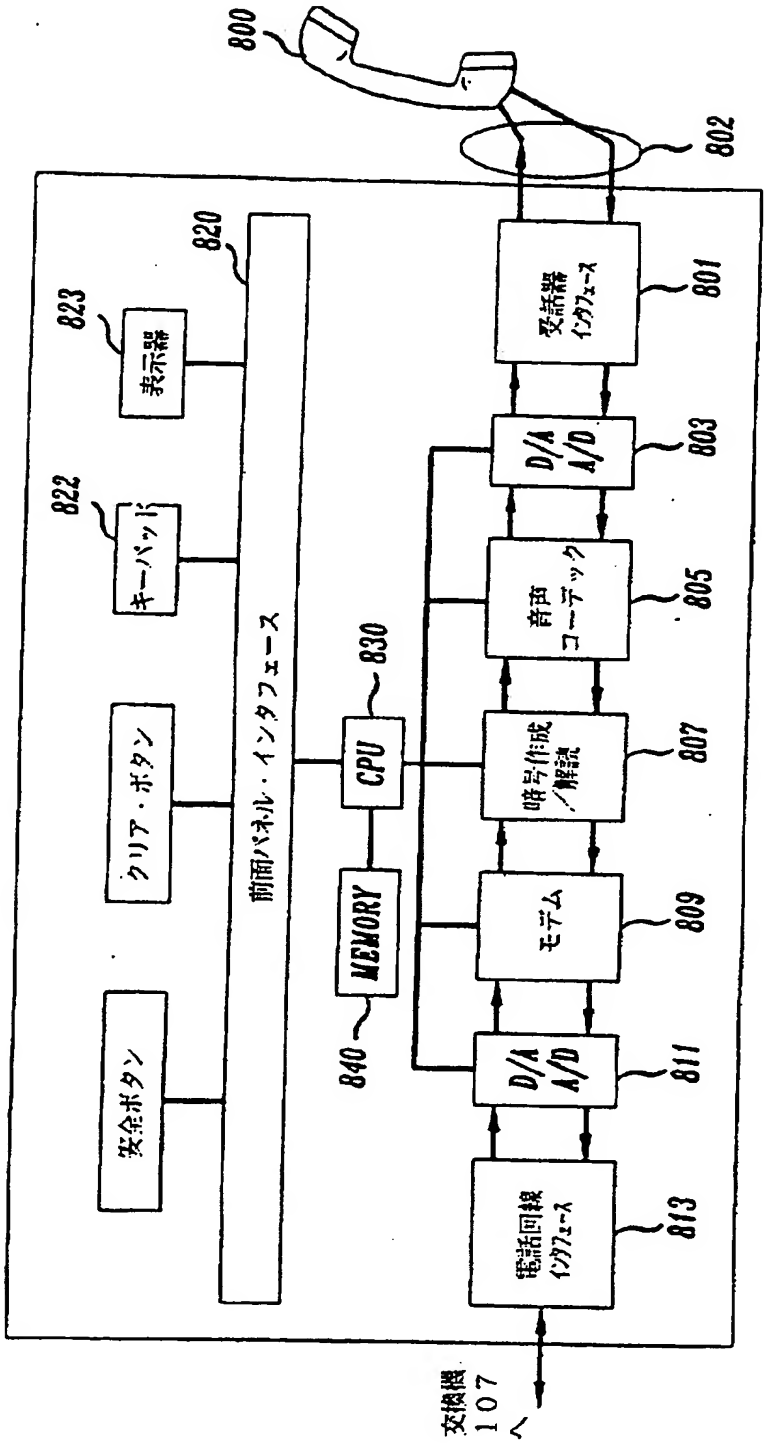
【図7】


101
CPE
301
304
SWITCH
151
暗号器／解読器
172
305
306
SWITCH
151
313
315
CONT
152
601
604
SWITCH
151
暗号器／解読器
174
605
606
SWITCH
613
314
CONT
152
307
308
SWITCH
151
102
CPE
第1種の安全
第2種の安全

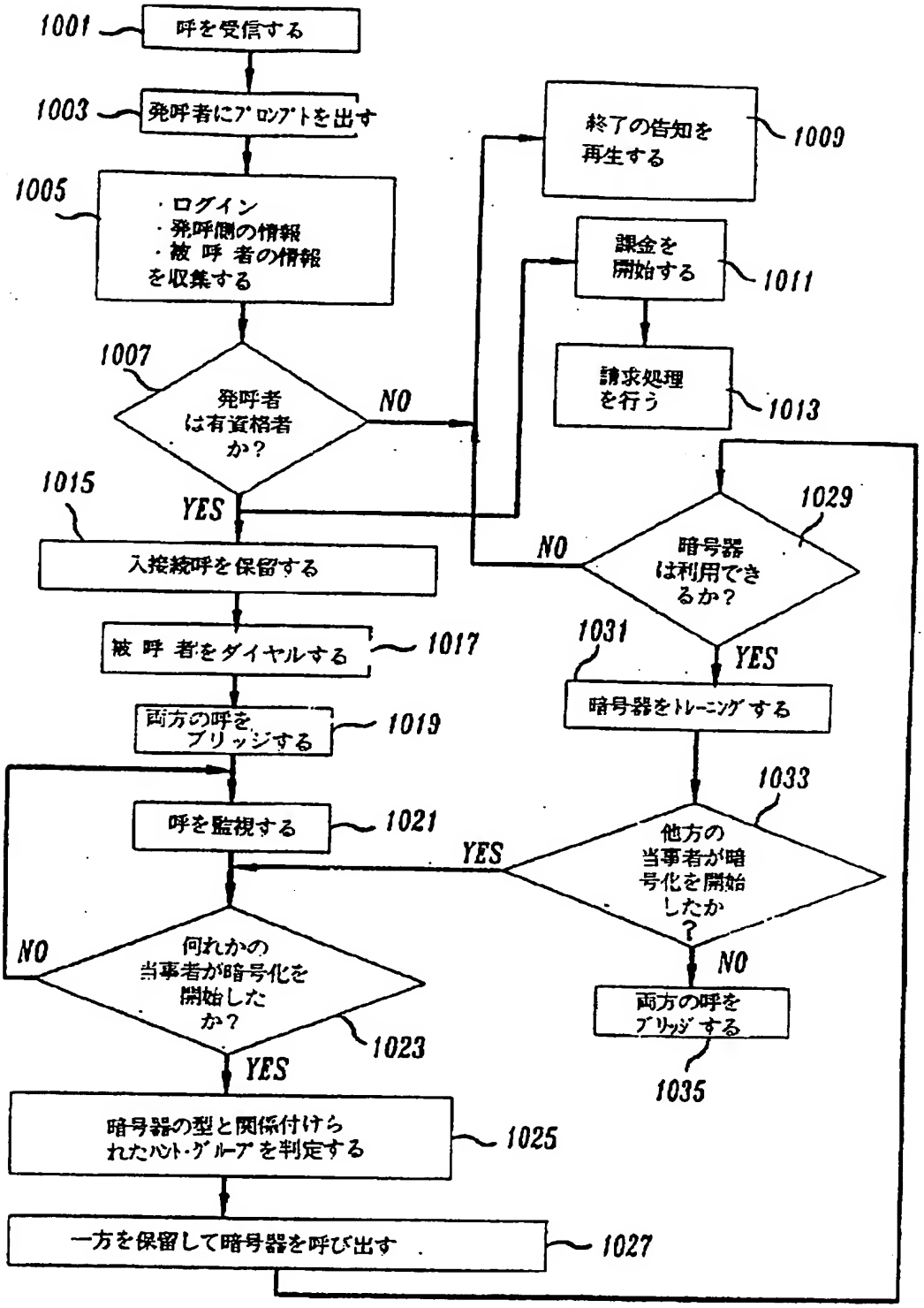
【図9】


920
信号インタフェース
930
CPU
940
MEMORY
交換機インタフェース
901
音声コーデック
905
暗号作成／解読
907
モデム
909
交換機インタフェース
913
スイッチ151へ
スイッチ151へ

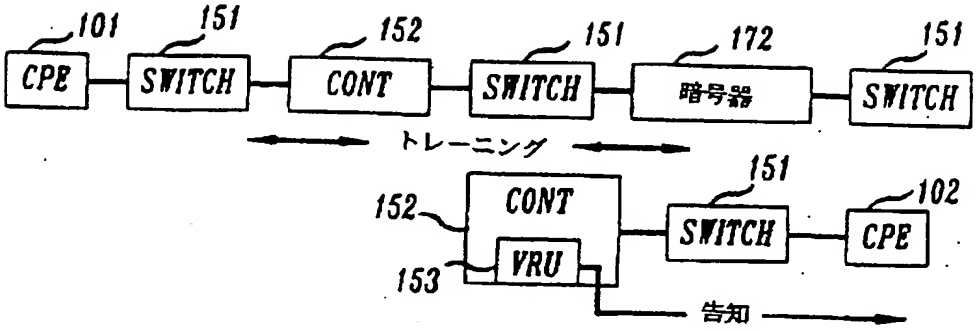
【図８】


800
802
受話器インタフェース
801
D/A
A/D
803
音声コーデック
805
暗号化/解読
807
モデム
809
D/A
A/D
811
電話回線インタフェース
813
交換機107へ
CPU
830
MEMORY
840
前面パネル・インタフェース
820
表示器
823
キーパッド
822
クリア・ボタン
安全ボタン

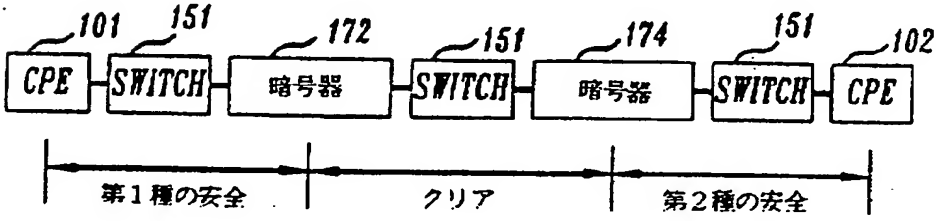
【図１０】


1001
呼を受信する
1003
発呼者にプロンプトを出す
1005
・ログイン
・発呼側の情報
・被呼者の情報
を収集する
1007
発呼者は有資格者か？
NO
YES
1009
終了の告知を再生する
1011
課金を開始する
1013
請求処理を行う
1015
入接続呼を保留する
1017
被呼者をダイヤルする
1019
両方の呼をブリッジする
1021
呼を監視する
1023
何れかの当事者が暗号化を開始したか？
NO
YES
1025
暗号器の型と関係付けられたハント・グループを判定する
1027
一方を保留して暗号器を呼び出す
1029
暗号器は利用できるか？
NO
YES
1031
暗号器をトレーニングする
1033
他方の当事者が暗号化を開始したか？
NO
YES
1035
両方の呼をブリッジする

【図１２】



【図１５】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/00				
Ｈ０４Ｑ　3/545		9076－5Ｋ		

(72)発明者　アンドリュー　エフ．バルファー
アメリカ合衆国　07046　ニュージャージー　マウンテン　レークス、ブルヴァード　85

(72)発明者　マイケル　エム．カプラン
アメリカ合衆国　01966　マサチューセッツ　ロックポート、オーシャン　アヴェニュー　4

(72)発明者　ブルース　イー．マクネア
アメリカ合衆国　07733　ニュージャージー　ホルムデル、アイロン　ヒル　ドライヴ　1

(72)発明者　キャロル　エー．ヴェグルジノヴィッツ
アメリカ合衆国　07733　ニュージャージー　ホルムデル，タコルサ　ドライヴ　29